V5.0 for DLP+ HyBoost

[Admin Manual V.1.4]

SOMANSA Copyright©2015 Somansa All rights reserved

Introduction

The contents of this Manual may be changed without prior notice to improve products and performance. The example companies, organizations, products, people and events depicted herein are fictitious. Any part of this Manual shall not be replicated, saved in a search system, introduced or transferred in any form or by any means (electronic, mechanical, copy machine, disk copy or otherwise), or for any purpose without the express approval of Somansa Co., Ltd..

Somansa Co., Ltd. holds patents, trademark rights, copyrights or other intellectual property rights covering subject matter in this Manual. Other than the rights provided to you by Somansa Co., Ltd. in accordance with any written license agreement, the provisions of this Manual shall not provide you any license regarding the patents, trademark rights, copyrights or other intellectual property rights.

©1997-2015 Somansa Co., Ltd. All rights reserved.
Privacy-i, Somansa is a registered trademark or trademark of Somansa Co., Ltd.
Other products and company names mentioned herein may be trademarks of their respective owners.

- Manufacturer (Supplier) Name: SOMANSA Co., Ltd.
- Address: 3003 N. First St., Suite 301, San Jose, California 95134
- Website Address: http://www.somansatech.com/
- Technical Support: Somansa Technical Support Team / (408) 701-1302 / support@somansatech.com Inquiries on Function/ On-Line Remote Assistance/ Off-Line Maintenance Support Requests / User Training Requests

[Remark]
The social security numbers on the UI screens included in the Manual are fabricated numbers for the purpose of providing realistic examples.

SOMANSA Copyright©2015 SOMANSA All rights reserved

Contents

1. Endpoint DLP: Privacy-i 8
1.1 Outline 8
1.1.1 What is Endpoint DLP, "Privacy-i"? 8
1.2 System Requirements 8
1.3 Package Configurations 9
1.4 Privacy-i Configuration Diagram 10
1.5 Product Information 11
1.5.1 First Release Date: March 25, 2015 11
1.5.2 Manual Configuration 11
2. Installation 12
2.1 Program Requirements 12
2.2 Installing Product 12
2.2.1 Installing Privacy-i Server Package 12
2.2.2 Installation Path 13
2.3 License 13
2.3.1 Issuance Procedure 13
2.3.2 What happens if the license is not renewed? 14
3. Configuration Manager 15
3.1 Running Configuration Manager 15
3.2 Configuration Manager Setup 15
3.3 Initial Connection Settings 15
3.3.1 Enter Password upon Initial Connection 15

SOMANSA Copyright©2015 SOMANSA All rights reserved

3.3.2 Setting Up a New Password 16
3.3.3 Enter Database Information 17
3.3.4 Enter Database Information 18
3.4 COMMON 20
3.4.1 Common Area Settings 20
3.4.1.1 Default Database Connection Settings 20
3.4.1.2 Product Schema Management 21
3.5 Privacy-i Settings 23
3.5.1 Privacy-i Server 23
3.5.1.1 Server Management 23
3.5.1.2 Advanced Options 23
3.5.1.3 License 23
3.5.2 Privacy-i Agent Update 25
3.5.2.1 Agent Update Configuration 25
3.5.2.2 View Agent Update History 29
3.6 DLP+ Center Settings 30
3.6.1 Server Management 30
3.6.2 Advanced Options 31
3.7 Preferences 33
3.7.1 Configuration Manager Administrator Account Information 33
3.7.2 Session Time 34
3.7.3 Time Synchronization 34
3.7.4 UID 35

SOMANSA Copyright©2015 SOMANSA All rights reserved

3.7.5 Access IP 35
3.7.6 Configuration Manager Initialization 35
3.7.7 Integrity Check 36
3.8 SYSTEM Audit Logs 36
3.9 Check Privacy-i Version 37
4. DLP+ Center 39
4.1 Dashboard 41
4.1.1 Discover 41
4.1.2 Endpoint 42
4.1.3 Settings 43
4.2 Reports 44
4.2.1 Discovery 46
4.2.1.1 PC 46
4.2.2 Endpoint 52
4.3 Incidents 55
4.3.1 Discover 55
4.3.1.1 PCs 55
4.3.2 Endpoint 56
4.4 Policy 59
4.4.1 Detection Rules 59
4.4.2 Discover 60
4.4.2.1 PC 60
4.4.3 Endpoint 63

SOMANSA Copyright©2015 SOMANSA All rights reserved

4.4.3.1 Copy Prevent+ 64
4.4.3.2 Print Prevent+ 66
4.4.3.3 Media Control 67
4.4.3.4 Policy Application Time 68
4.4.4 Connections 68
4.4.5 Apply to Targets 70
4.4.5.1 PCs 70
4.5 Manage 72
4.5.1 Identifiers 72
4.5.1.1 Pattern 72
4.5.1.2 File Format 73
4.5.1.3 Attributes 75
4.5.2 Admin Action 76
4.5.2.1 PC 76
4.5.3 Alerts/Notification 78
4.5.3.1 Reports 78
4.5.4 Users 81
4.6 System 85
4.6.1 Logs 85
4.6.1.1 System Logs 85
4.6.2 Admin 87
4.6.3 Tools 89
4.6.3.1 Uninstall Password Generator 89

SOMANSA Copyright©2015 SOMANSA All rights reserved

4.6.4 View Privacy-i Version 89

5. Uninstalling Privacy-i 90

6. FAQ 91

7. Definition of Terms 94

SOMANSA Copyright©2015 SOMANSA All rights reserved

1. Endpoint DLP: Privacy-i

1.1 Outline

1.1.1 What is Endpoint DLP, "Privacy-i"?

Endpoint DLP, "Privacy-i", is a tool that automatically scans and locates sensitive data stored on a PC which is designated to be deleted or blocked from transferring via USB drives, removable storage, Media, Applications, and Printing based on content-aware policies.

1.2 System Requirements

Please refer to [Table 1-2] for the correct operating system version on which to install the Server, Administration Console and Agent.

[TABLE 1-1] OPERATING SYSTEM IDENTIFICATION

Category	Operating System
Privacy-i Server DLP+ Center Configuration Manager	CentOS6.4_x64 or higher (Kernel 2.6.x or higher)
Privacy-i Agent (Windows)	Windows 7 (x86/x64) Edition - Home Premium - Professional - Ultimate - Enterprise Windows 8 (x86/x64) Windows 8 Pro (x86/x64) Windows 8 Enterprise (x86/x64)

Below are the hardware requirements to install the Server, Administration Console and Agent.

[TABLE 1-2] MINIMUM HARDWARE REQUIREMENTS TO INSTALL PRIVACY-I

Category	Hardware and Software Requirements	
Privacy-i Server	CPU	Intel Quad Xeon 3.1GHz * 1 +

SOMANSA Copyright©2015 SOMANSA All rights reserved

DLP+ Center Configuration Manager	HDD	500GB * 2 (raid1) +
	MEMORY	8GB +
Privacy-i Agent	CPU	Intel Core 2 1.6Ghz
	HDD	3 GB + Free space
	MEMORY	1GB +
※ Number of simultaneous users of Privacy-i Agent: Recommended to be limited to 3000 Users per server. Dispersed operations to multiple servers are required when there are more than 3000 Users.		

1.3 Package Configurations

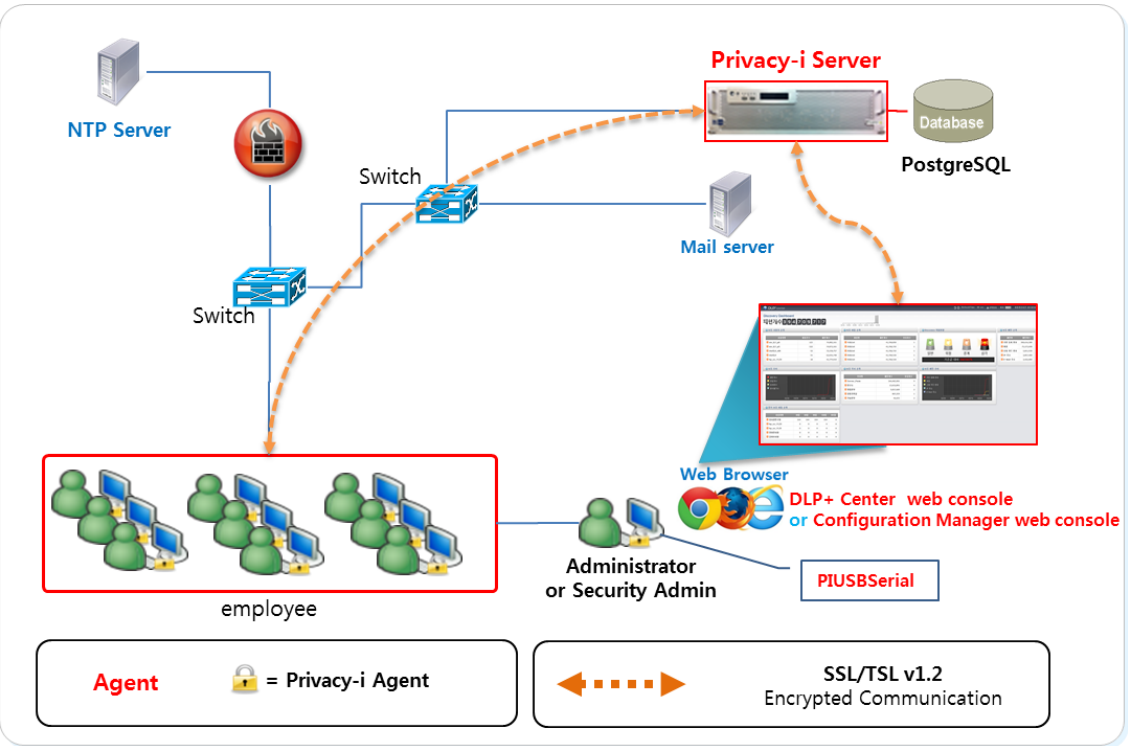
Privacy-i V5.0 for DLP+ HyBoost package is configured as shown in [Table 1-4].

[TABLE 1-3] PRIVACY-I PACKAGE CONFIGURATION ITEMS

Category	Qty.	Remark
Privacy-i Server Package	1	Server Application
Privacy-i Agent Package	1	Agent Application to be installed on a user's computer
Admin/User Manual	1	Admin Manual
Software License Certificate	1	License Certificate to allow the use of the software

SOMANSA Copyright©2015 SOMANSA All rights reserved

1.4 Privacy-i Configuration Diagram



(FIGURE 1-1) PRIVACY-I SYSTEM CONFIGURATION DIAGRAM

☞ **"Privacy-i V5.0 for DLP+ HyBoost" runs tasks according to the following procedures.**

① Install the agent on a PC to inspect whether it contains sensitive data or not.

② The agent periodically searches data on the local disk of a host.

③ The agent sends a search result to the server, and the result is saved on the HDD for log storage.

④ The user can run a self-diagnosis on the agent to check whether the PC retains any data or not. Option.

⑤ According to the Admin Policy, the agent controls the external interfaces of a host (USB, Print, CD/DVD, Bluetooth, Wired/ Wireless LAN, etc.) or checks the data that is transmitted to run the function of data leakage control.

☞ **Admin runs the following tasks through the Configuration Manager.**

① Connect to the database to save logs and policies.

② Use PostgreSQL 9.3 as a database for storing data such as logs and policies. And, use TCP/IP-based data communication when the Privacy-i Server and DLP+ Center communicate with the database.

③ Set the HDD capacity on the DB logs to prevent losing logs when they become full.

④ Register the Privacy-i license.

☞**Admin runs the following tasks through the DLP+ Center.**

SOMANSA Copyright©2015 SOMANSA All rights reserved

① Set the Data Pattern to be based on when the agent searches for data on a user PC.
② Create or edit another admin or user account.
③ View the searched data and analyze Data Trends in a company. Alert each user, delete a file.

Tomcat Server, which is operated by the server, is configured with 3 components, and includes the port as follows.

[TABLE 1-4] SERVICE PORT BY CONFIGURATION MODULE

Component	Port	Remark
DLP+ Center	443	
Privacy-i Server		
Configuration Manager		

1.5 Product Information

1.5.1 First Release Date: March 25, 2015

1.5.2 Manual Configuration

Manual consists of two parts, an Admin Manual and a User Manual. The Admin Manual includes instructions and descriptions of configuration, installation and usage of the server. The User Manual includes instructions and descriptions of configuration, installation and usage of the agent.

- Admin Manual: Privacy-i V5.0 for DLP+ HyBoost Admin Manual V1.4.docx
- User Manual: Privacy-i V5.0 for DLP+ HyBoost User Manual V1.4.docx

SOMANSA Copyright©2015 SOMANSA All rights reserved

2. Installation

2.1 Program Requirements

To install Privacy-i V5.0 for DLP+ HyBoost product, the programs below are required.

[TABLE 2-1] ENVIRONMENTAL CONDITIONS INSTALLER

TABLE 2-2

Program	Version	Remark
PostgreSQL	9.3	Database
gcc-c++	4.4.7	Compiler
Java Runtime Environment (JRE)	1.7	Runtime Environment

Recommendations

✓ When creating a PostgreSQL account, it is recommended to create and add a Database Admin account, rather than using the Default account.

2.2 Installing Product

2.2.1 Installing Privacy-i Server Package

To run the Privacy-i Server Package of Privacy-i V5.0 for DLP+ HyBoost, run the '**Privacy-i_V5.0_for_DLP+_HyBoost_Install.BIN**' installation file. (※ before installing the product, PostgreSQL must be installed. Please note that the package cannot be installed if PostgreSQL is not installed.) Run the Package as follows. (Please check the file permissions when running the Package.)

#sh Privacy-i_V5.0_for_DLP+_HyBoost_Install.BIN

During installation, when the following message is received, enter the IP of a PC where the Security Admin can connect to the Configuration Manager. Please note that the Configuration Manager can be only connected from one registered PC.

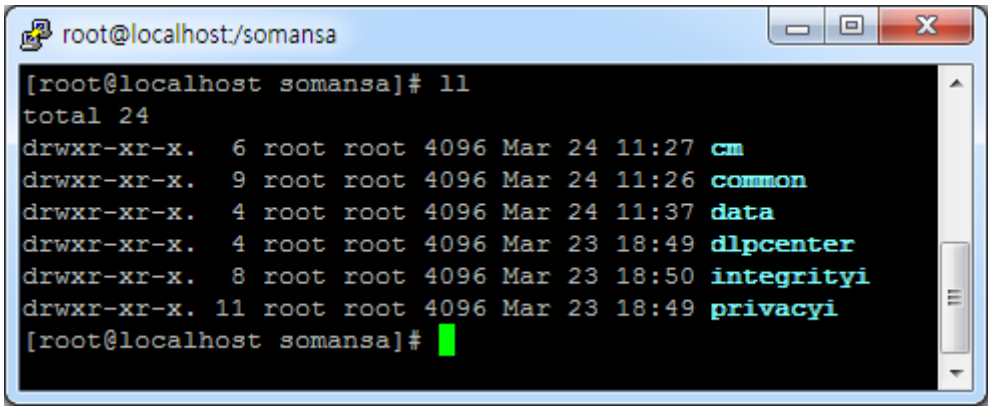
SOMANSA Copyright©2015 SOMANSA All rights reserved

Please, input the IP Address of the desktop to connect Configuration Manager

192.168.10.171 (Information that the User must enter)

2.2.2 Installation Path

When installation of Privacy-i 5.0 for DLP+ HyBoost Package is complete, the product is installed on the /somansa path as shown below (Figure 2-1).


root@localhost:/somansa
[root@localhost somansa]# ll
total 24
drwxr-xr-x. 6 root root 4096 Mar 24 11:27 cm
drwxr-xr-x. 9 root root 4096 Mar 24 11:26 common
drwxr-xr-x. 4 root root 4096 Mar 24 11:37 data
drwxr-xr-x. 4 root root 4096 Mar 23 18:49 dlpcenter
drwxr-xr-x. 8 root root 4096 Mar 23 18:50 integrityi
drwxr-xr-x. 11 root root 4096 Mar 23 18:49 privacyi
[root@localhost somansa]#

(FIGURE 2-1) INSTALLATION PATH SETTINGS SCREEN

When installation of the Privacy-i Server is complete, connect to the Configuration Manager, extract the UID of the Server, and apply for issuance of a License by contacting a Somansa Support Team member. The connecting address to the Configuration Manager is as follows.

https://IP_ADDR/cm

2.3 License

2.3.1 Issuance Procedure

STEP 1

Connect to the Configuration Manager through a web browser and check the UID preferences. With the extracted UID, request for "License Issue" A License Key will be sent by E-mail.

STEP 2

Copy the two License files (privacyi.license, privacyi.license.serial) sent by E-mail to the '/somansa/common/license' folder.

STEP 3

The Registered License can be checked in the Configuration Manager > Privacy-i > License tab.

SOMANSA Copyright©2015 SOMANSA All rights reserved

License Issuance

When all of the steps above are completed, the license application is complete. The License will be sent by E-mail, and 2 files including privacyi.license, and privacyi.license.serial will be attached. Copy the attached files to the {Program_Installation Folder}₩SomansaFramework₩Common2 folder to control the Control Panel.

2.3.2 What happens if the license is not renewed?

If a product license agreement has expired and not renewed, the product will not update. In addition, the latest security patch files cannot be received, and server operation cannot be controlled when Privacy-i Server is down. Therefore, please renew a license when it has expired.

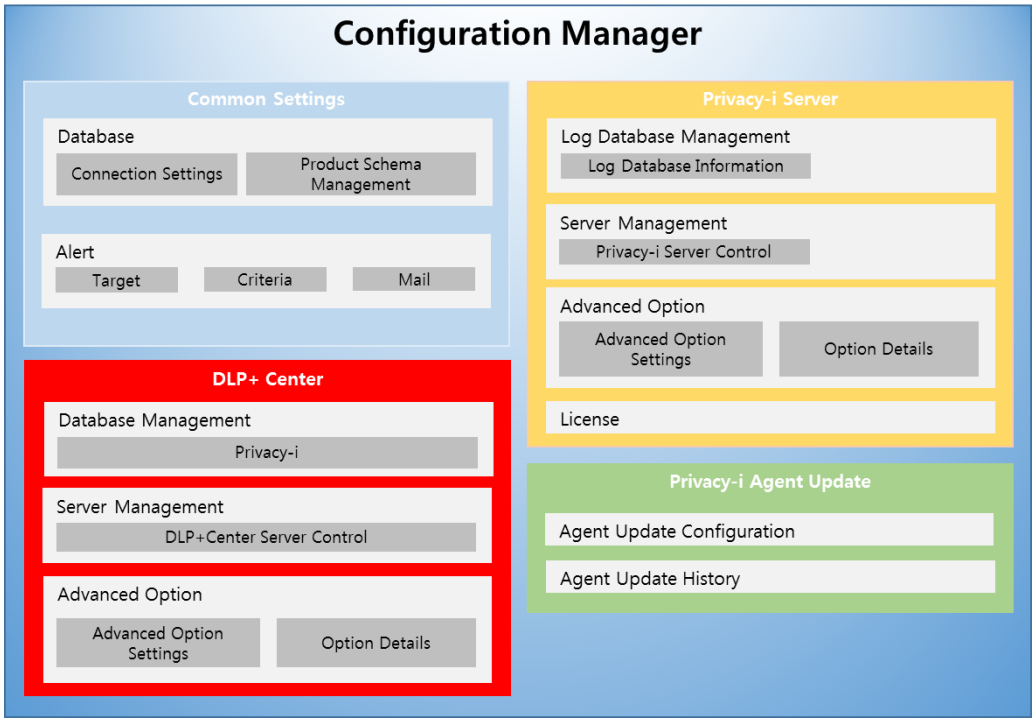
SOMANSA Copyright©2015 SOMANSA All rights reserved

3. Configuration Manager

3.1 Running Configuration Manager

Run the Configuration Manager through a web browser. The first Security Admin password is provided, and should be changed after login. If the password is forgotten, please contact the SOMANSA Support Team.

3.2 Configuration Manager Setup



(FIGURE 3-1) CONFIGURATION MANAGER DIAGRAM

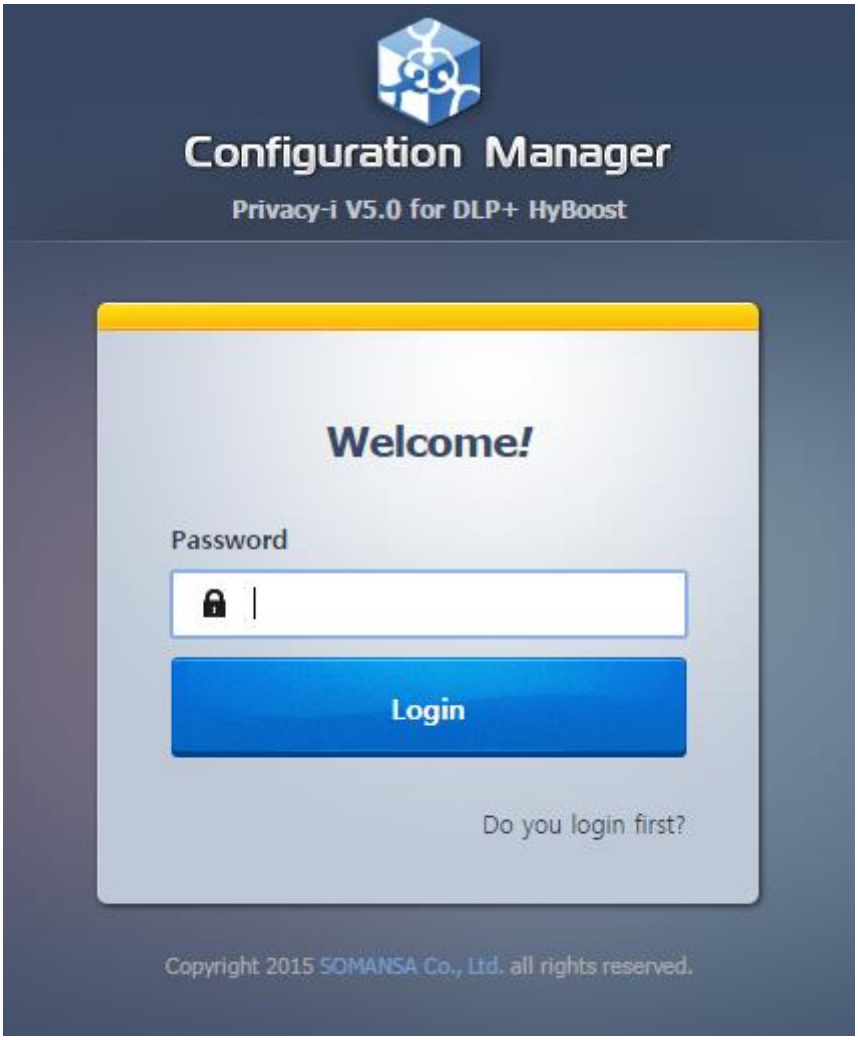
The Configuration Manager is set up as shown in (Figure 3-1). The Configuration Manager provides Common Area Settings, Privacy-i, DLP + Center, Preferences, etc.

3.3 Initial Connection Settings

3.3.1 Enter Password upon Initial Connection

When logged in to Configuration Manager, the login page will appear as below (Figure 3-2). The admin account in Configuration Manager is "Security Admin", and only one account is available. Therefore, do not enter a separate ID. Enter the default password upon initial connection, and log in with the "Security Admin".

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 3-2) CONFIGURATION MANAGER LOGIN SCREEN

☞ Effective Input Field Range

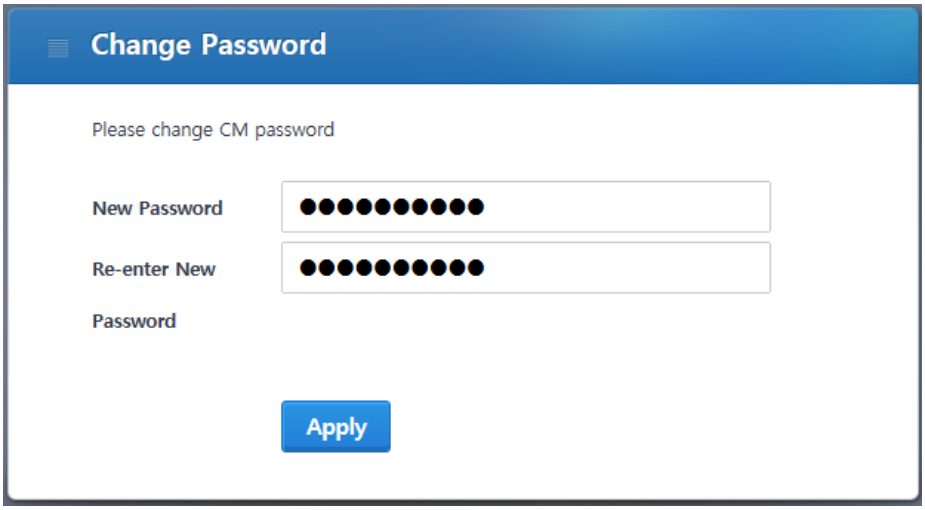
[TABLE 3-1] EFFECTIVE INPUT FIELD RANGE UPON LOGIN

Item	Effective Range	Character	Failure Message
Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter password.

3.3.2 Setting Up a New Password

After entering a password, the Change Password screen will appear (Figure 3-3). Set up a new password for the Security Admin in the Configuration Manager.

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 3-3) SETTING UP A NEW PASSWORD IN THE CONFIGURATION MANAGER SCREEN

☞ Effective Input Field Range

[TABLE 3-2] EFFECTIVE INPUT FIELD RANGE UPON LOGIN

Item	Effective Range	Character	Failure Message
New Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter new password.
Confirm a New Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter password again.

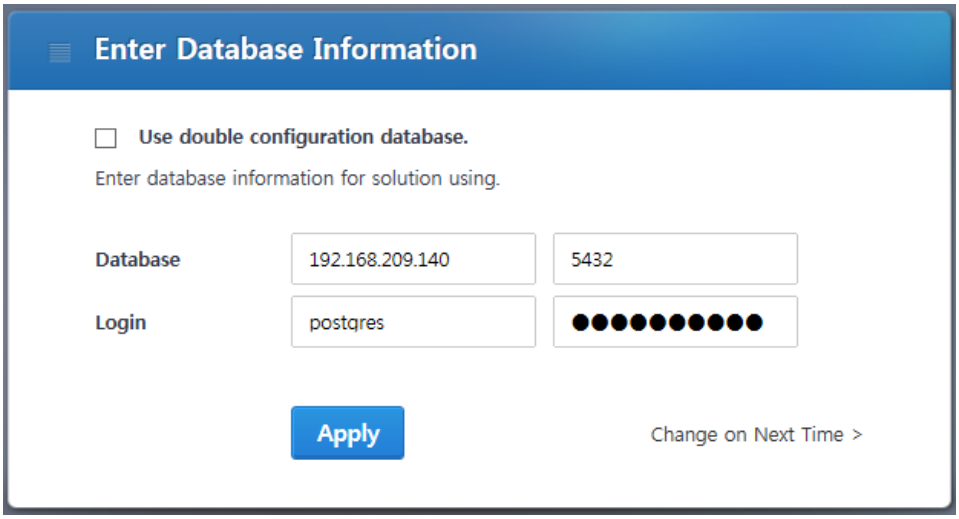
Recommendations

✓ Password should have at least 9 characters and include English letters, numbers and special characters.

3.3.3 Enter Database Information

Enter database information for "Privacy-i V5.0 for DLP+" on this screen. Enter the database accessible IP/ Port/ Account.

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 3-4) ENTER DATABASE INFORMATION IN THE CONFIGURATION MANAGER

☞ Item Description

① Enter Database Information: Enter the default database information of the server. If a database with a redundancy configuration is used, enter the information for an existing configured server where the database is installed.

☞ Effective Input Field Range

[TABLE 3-3] EFFECTIVE INPUT FIELD RANGE UPON CONNECTION TO THE DEFAULT DATABASE

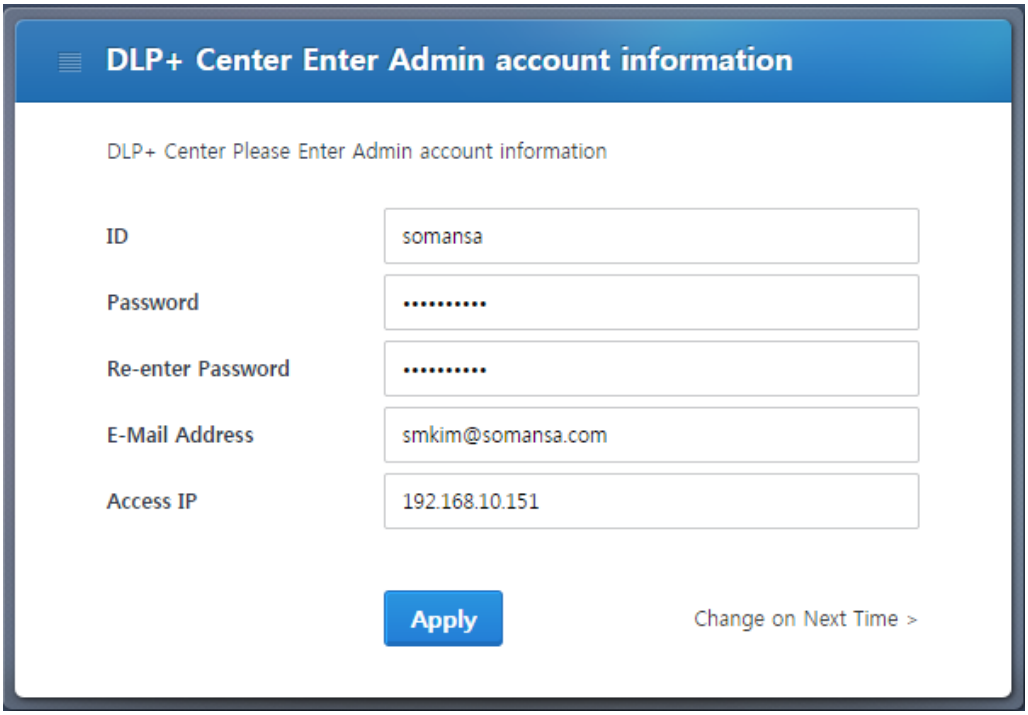
Item	Effective Range	Character	Failure Message
Database (IP)	15	Numbers, special characters (.)	Enter the IP of the default DB.
Database (Port)	1~65536	Numbers	Enter the port of the default DB.
Login (ID)	5~256	Letters	Enter the login ID of the default DB.
Login (Password)	9~70	Numbers, letters, special characters	Enter the password of the default DB.

3.3.4 Enter Database Information

Set the admin account information for the DLP+ Center on this screen. Specify the admin

SOMANSA Copyright©2015 SOMANSA All rights reserved

account ID and password of the DLP+ Center, and configure the "Access IP" with the IP that the admin account has access to. In an environment with IP other than the Access IP, connection is not possible. (※ please note that it should be reinstalled or contact a SOMANSA Support Team member if Access IP is lost.)



(FIGURE 3-5) ENTER SECURITY ADMIN ACCOUNT INFORMATION FOR CONFIGURATION MANAGER DLP+ CENTER

☞ Effective Input Field Range

[TABLE 3-4] EFFECTIVE INPUT FIELD RANGE UPON LOGIN

Item	Effective Range	Character	Failure Message
ID	5~100	Letters	Enter the DLP+ Center admin ID.
Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter the DLP+ Center admin password.
Re-enter Password	9~41	Numbers, uppercase/ lowercase letters, special characters	Enter the DLP+ Center admin password again.
Access IP	15	Numbers, special characters (.)	Enter the valid IP of the DLP+ Center admin.

SOMANSA Copyright©2015 SOMANSA All rights reserved

Recommendations

✓ Password should have at least 9 characters and include English letters, numbers and special characters.

3.4 COMMON

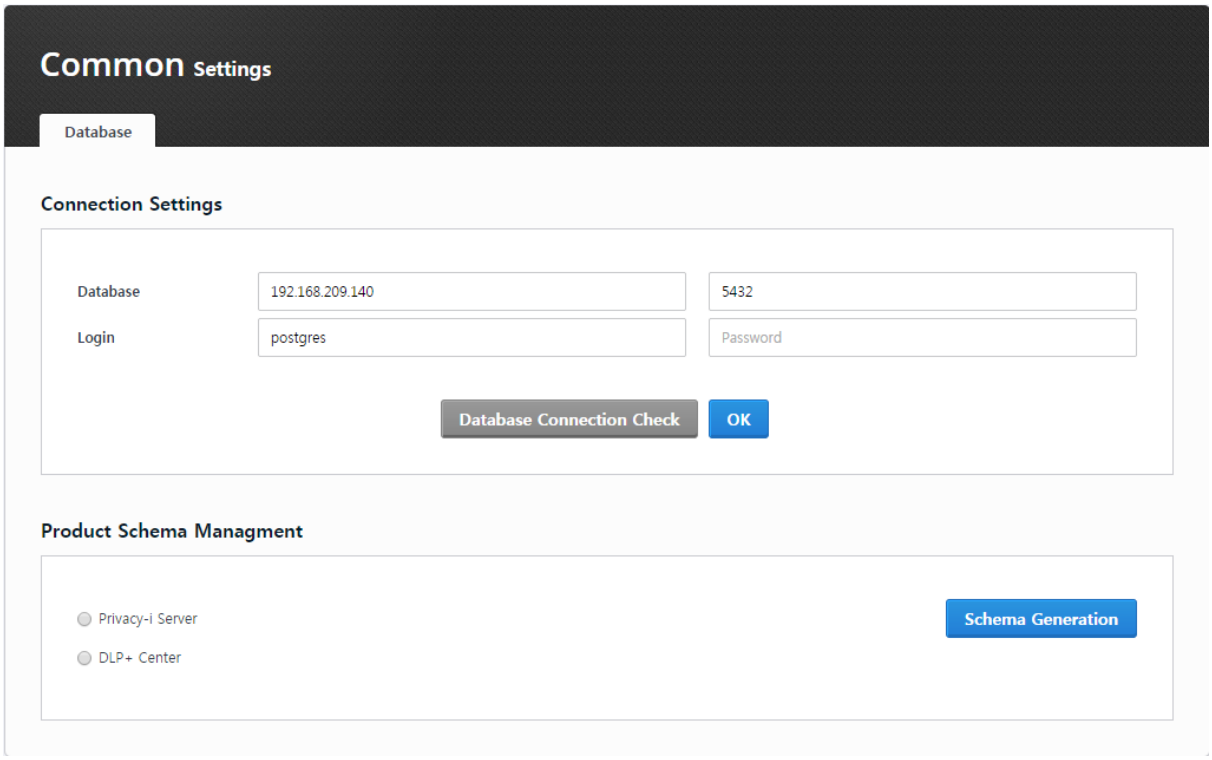
3.4.1 Common Area Settings

Once the initial Configuration Manager setup is complete, the "Common Area Settings" menu appears. This initial page appears upon re-login to the Configuration Manager. The Common Items provide the Default Database Settings, Log Forgery/ Falsification Prevention, and Alert Settings for disk space of "Privacy-i V5.0 for DLP+HyBoost".

3.4.1.1 Default Database Connection Settings

(Figure 3-6) is a screen where a common database connection can be set up. The common database shows input information in the "3.3.3 Enter Database Information" during initial installation. If the "Privacy-i V5.0 for DLP+ HyBoost" database information is modified, it updates the information through "Default Database Connection Settings".

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 3-6) COMMON AREA SETTINGS SCREEN

After entering common database connection information, the session status can be checked through "Check Database Connection". If the connection failure window appears, please check if the account information is entered incorrectly, or the service status of the database.

☞ Effective Input Field Range

[TABLE 3-5] EFFECTIVE INPUT FIELD RANGE UPON THE DEFAULT DATABASE CONNECTION

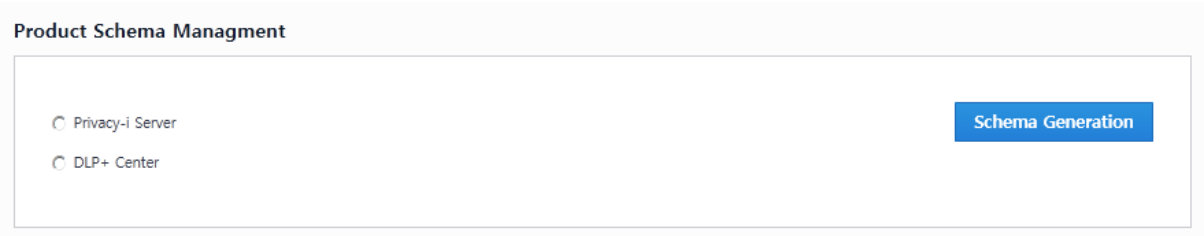
Item	Effective Range	Character	Failure Message
Database (IP)	15	Numbers, special characters (.)	Enter the IP of the DB.
Database (Port)	1~65536	Numbers	Enter the port of the DB.
Login (ID)	5~256	Letters	Enter the login ID.
Login (Password)	9~70	Numbers, letters, special characters	Enter the password of the DB.

3.4.1.2 Product Schema Management

After the initial preference task, a task must be run through "Create Schema". This creates a database that is needed to run Privacy-i Server, DLP+ Center, and the Schema is created in the

SOMANSA Copyright©2015 SOMANSA All rights reserved

database entered in the "Default Database Connection Settings". When "Create Schema" is clicked, a notification window that displays, "If such information exists in the database, it will be removed. Do you want to continue?" is generated, and the initial data required for operating the selected Schema is created. Please note that the database information will be initialized if Create Schema is continued while operating solutions.



(FIGURE 3-7) PRODUCT SCHEMA MANAGEMENT SCREEN

SOMANSA Copyright©2015 SOMANSA All rights reserved

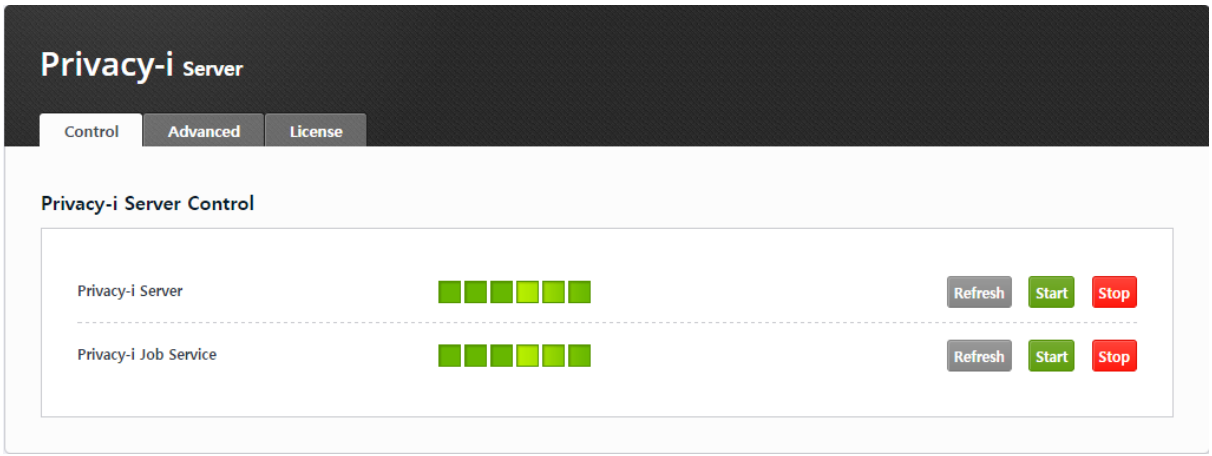
3.5 Privacy-i Settings

Privacy-i Running Status, Log Settings, License and Advanced Options are provided.

3.5.1 Privacy-i Server

3.5.1.1 Server Management

The status of the Privacy-i Server and its operation can be set. As shown in (Figure 3-13), Restart, Start and Stop functions for the Privacy-i Server are provided.



(FIGURE 3-8) PRIVACY-I SERVER CONTROL

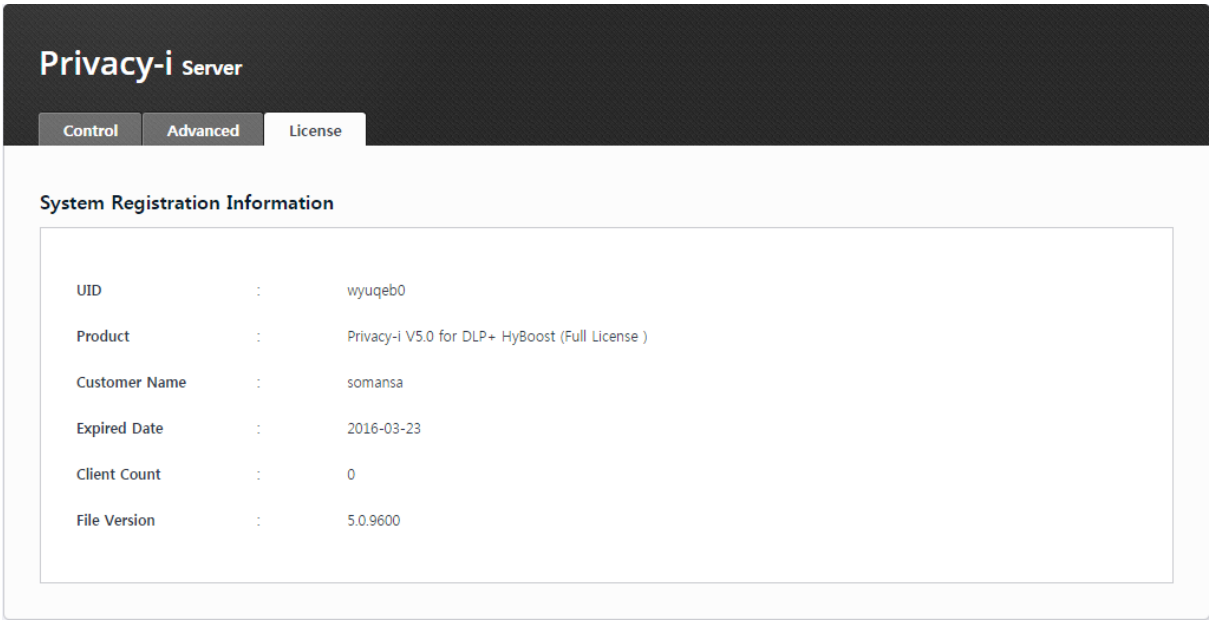
3.5.1.2 Advanced Options

Advanced Options can lead to errors in Privacy-i operation when used incorrectly by a non-experienced user. We recommend not modifying the Advanced Options unless modification is absolutely necessary since default values are set. Please contact the Support Team for more details.

3.5.1.3 License

UID/License expiration date/ number of users, etc. are displayed (see Receive License Issuance). Place the License received from the SOMANSA in the /somansa/common/license folder to register the license as above. If the valid date of the License is expired or a License from another server is copied, main functions such as Data Pattern Update will not work. (See License Issuance)

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 3-9) PRIVACY-I LICENSE SCREEN

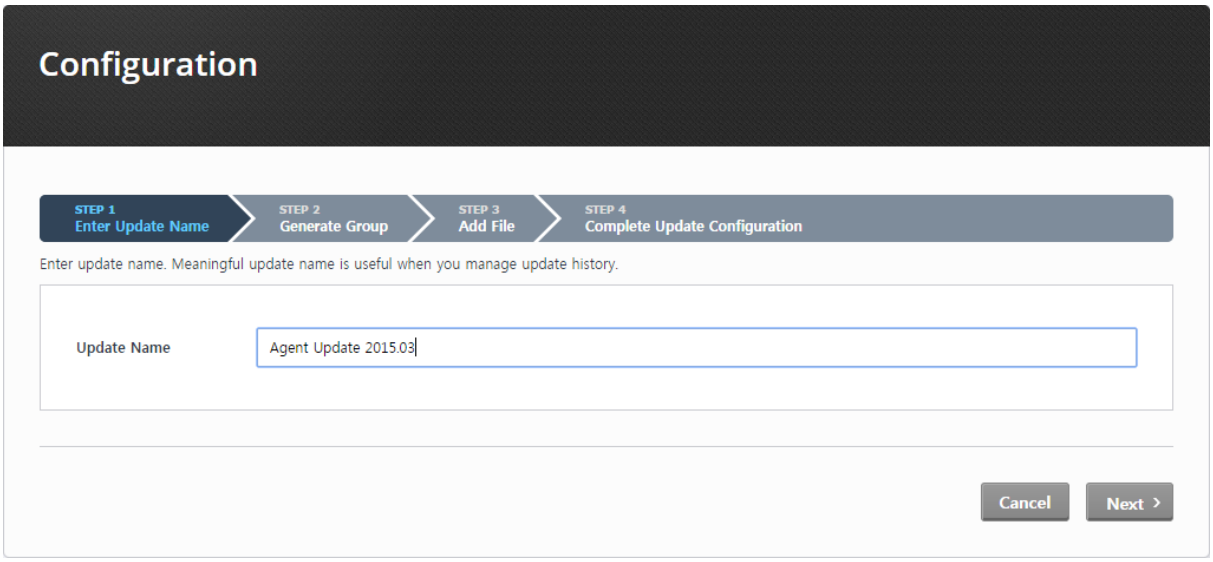
SOMANSA Copyright©2015 SOMANSA All rights reserved

3.5.2 Privacy-i Agent Update

3.5.2.1 Agent Update Configuration

Step 1. Enter Update Name

Enter a name for the update process task. (Example: Agent Update 2015.03)

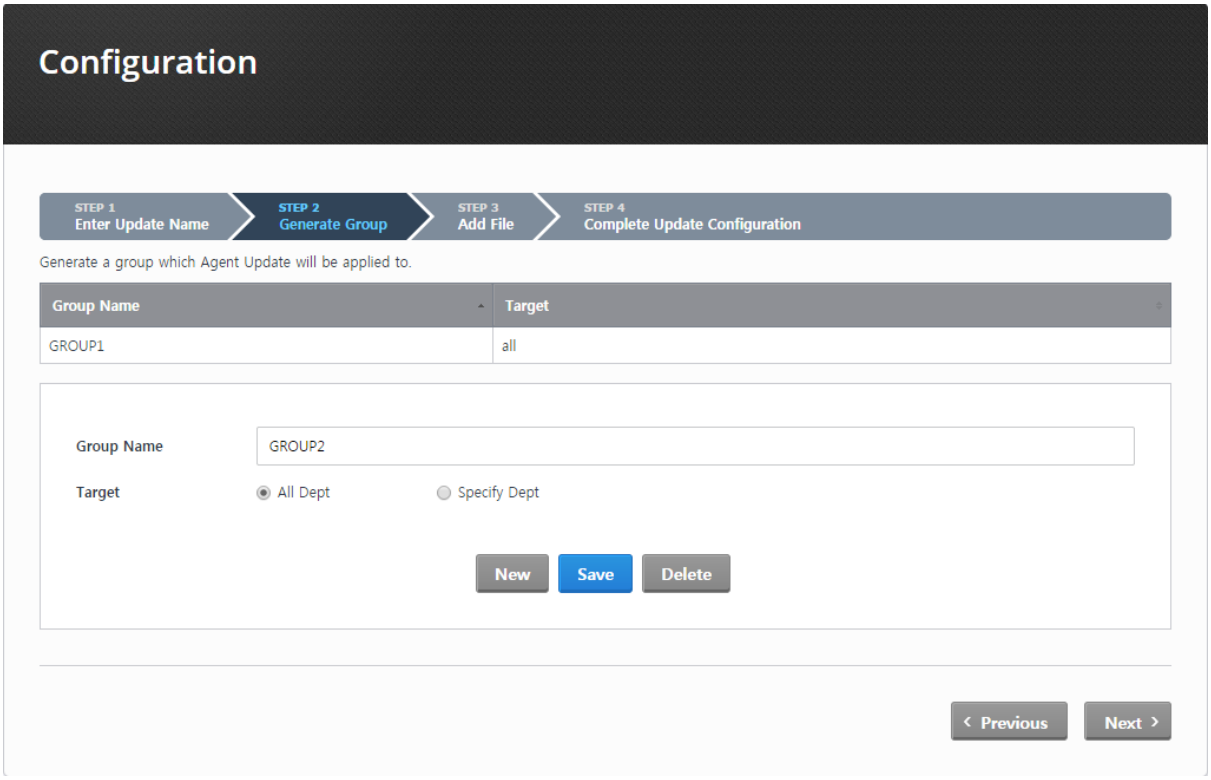


(FIGURE 3-10) ENTER UPDATE NAME SCREEN

Step 2. Generate Group

Generate an update group. One or more group(s) must be specified, and can be categorized according to the characteristics of the module. In addition, the target to be applied to the group can be specified as a whole or selectively based on the user information.

SOMANSA Copyright©2015 SOMANSA All rights reserved

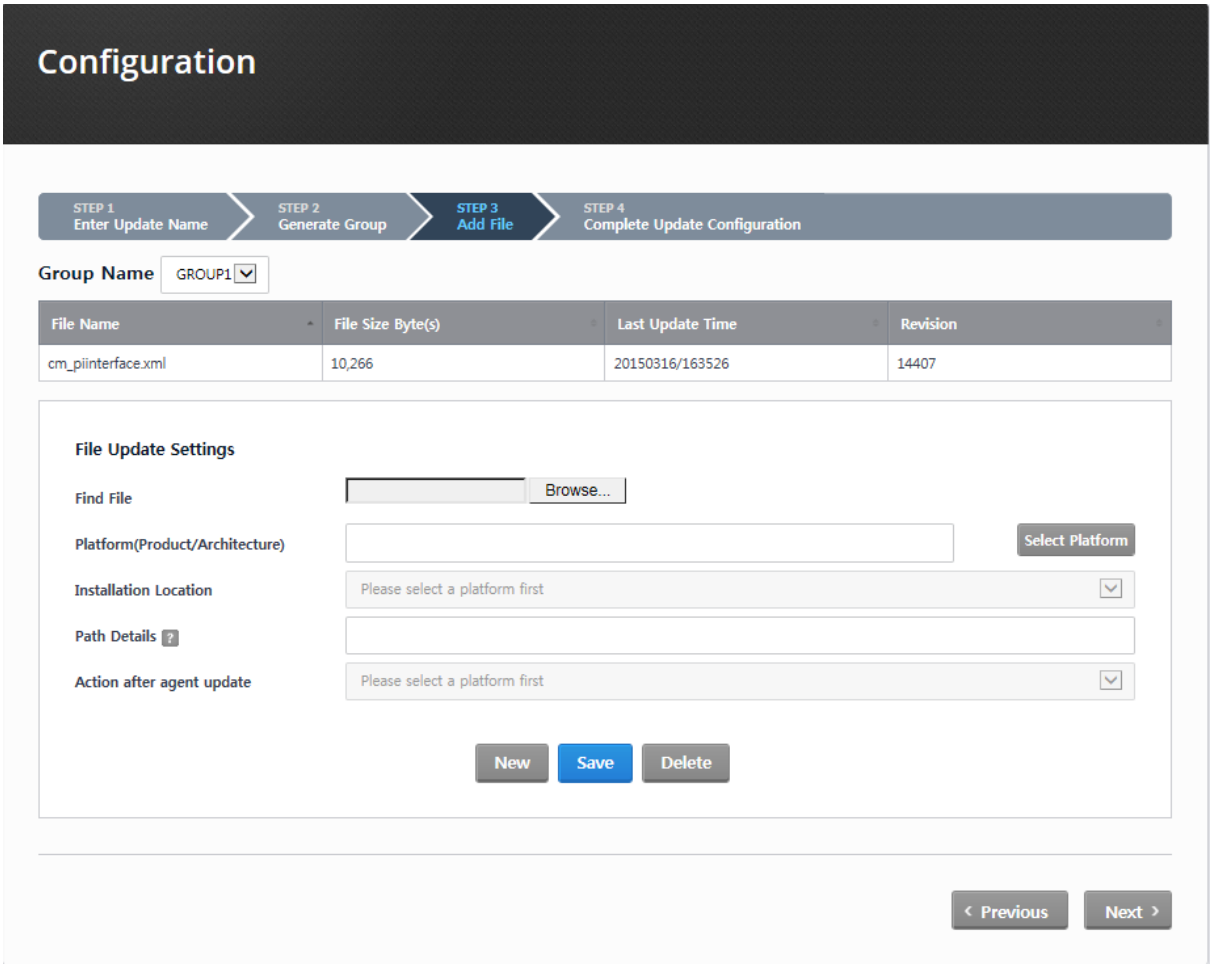


(FIGURE 3-11) GROUP GENERATION SCREEN

Step 3. Add File

Add a file to update. On a platform, OS type and architecture name (x86. x64) can be selected. Installation location can be selected from the Privacy-i Agent installation folder, Privacy-i Data folder, Windows folder and System32 folder; and a detailed path can be entered. (Omit / before and after the entered path) 'No Action', 'Create Service', 'Run', 'Register Registry' and 'Restart Privacy-i Agent' can be selected for the following action.

SOMANSA Copyright©2015 SOMANSA All rights reserved

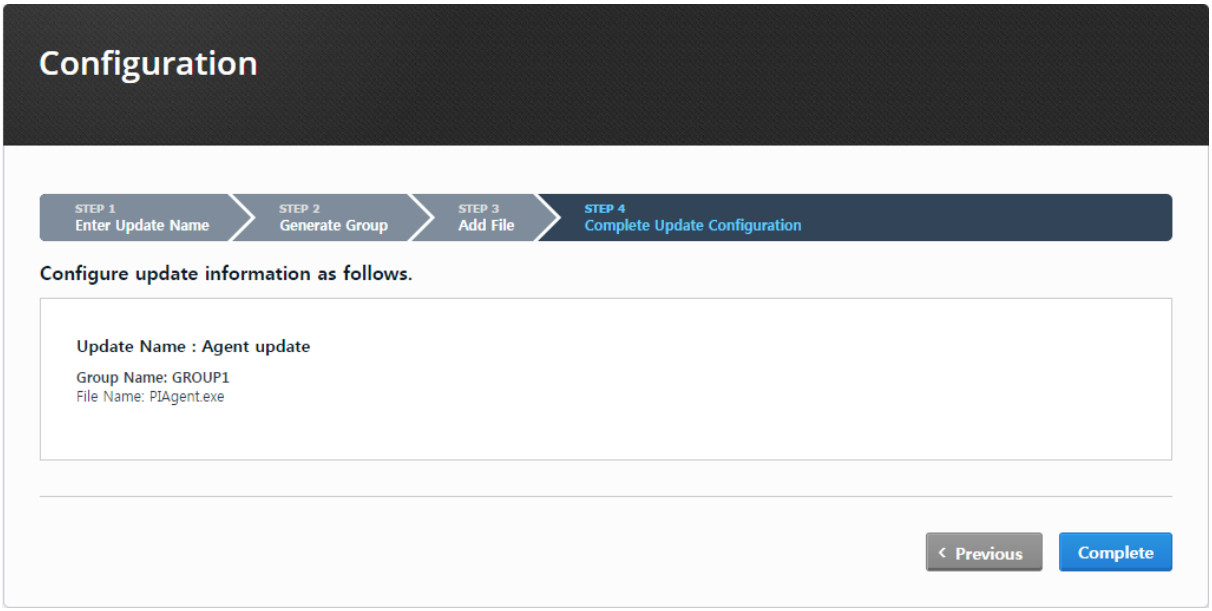


(FIGURE 3-12) ADD FILE SCREEN

Step 4 Completed Update Configuration

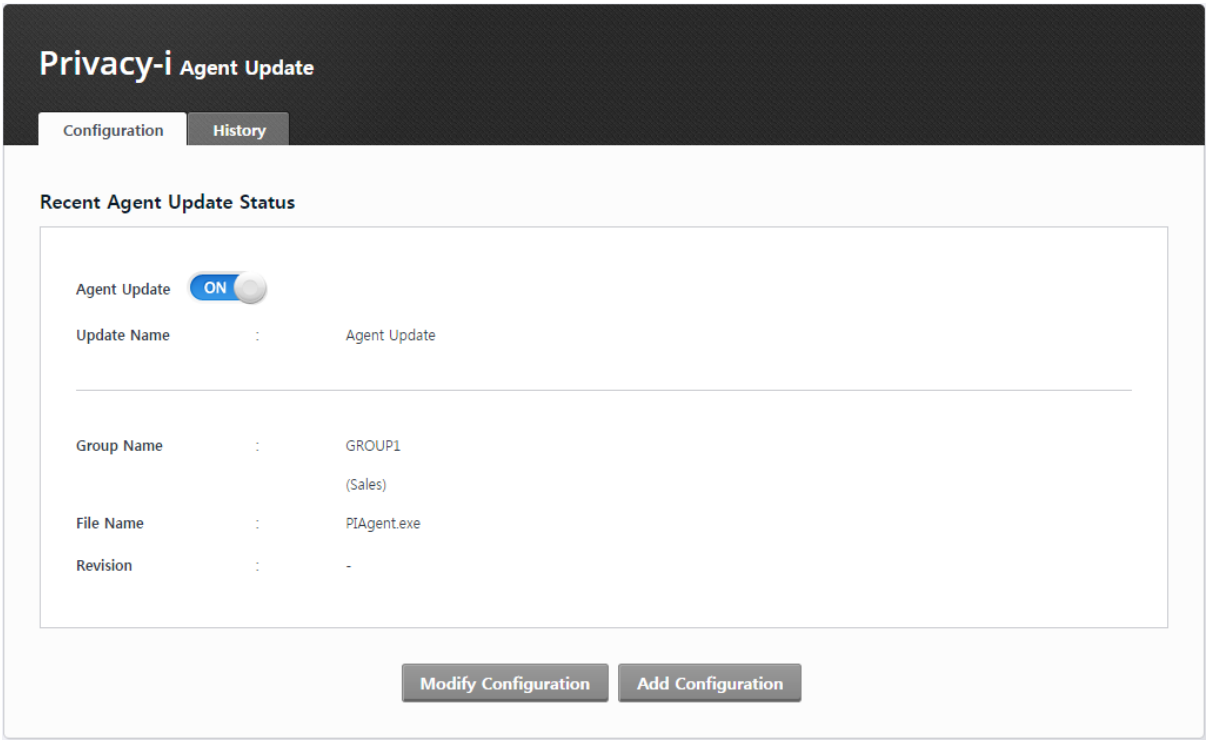
Configured update information can be viewed.

SOMANSA Copyright©2015 SOMANSA All rights reserved



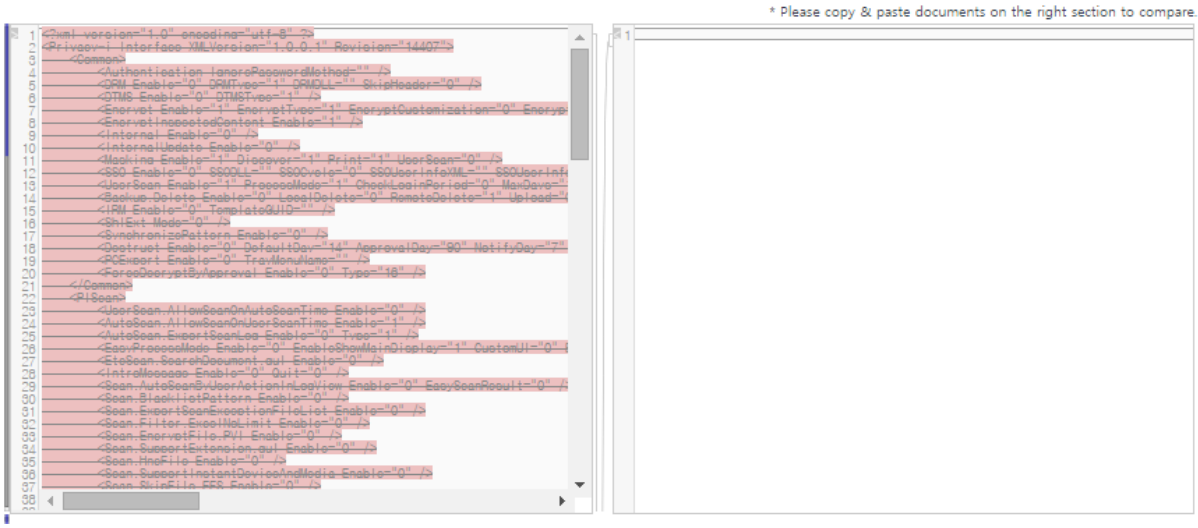
(FIGURE 3-13) COMPLETED UPDATE CONFIGURATION SCREEN

When update configuration is complete, the updated information is saved as an xml file. When a saved xml file, existing xml or xml to be configured needs to be checked, it can be compared using the 'diff' button.



(FIGURE 3-14) DIFF BUTTON

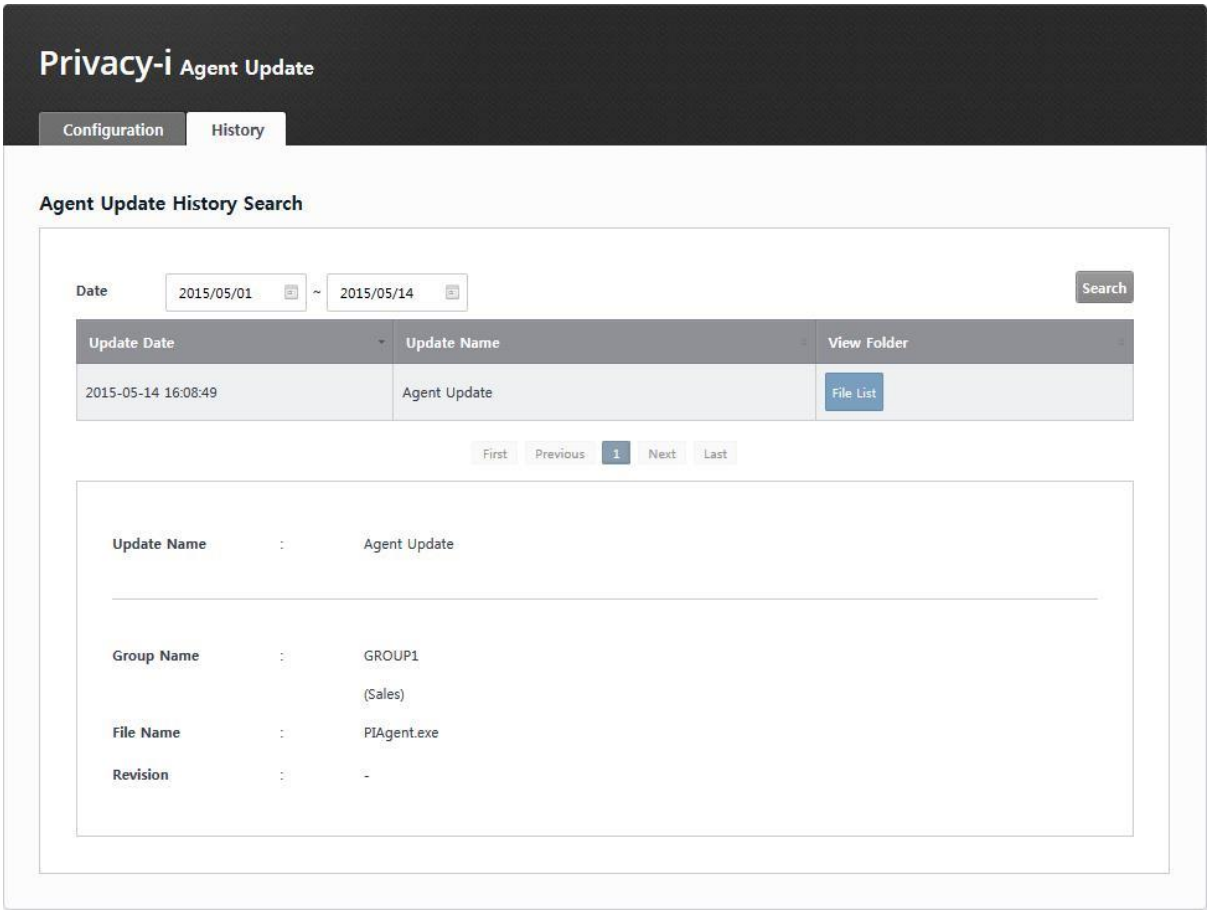
SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 3-15) XML CONTENT COMPARISON SCREEN

3.5.2.2 View Agent Update History

History of agent update can be viewed.



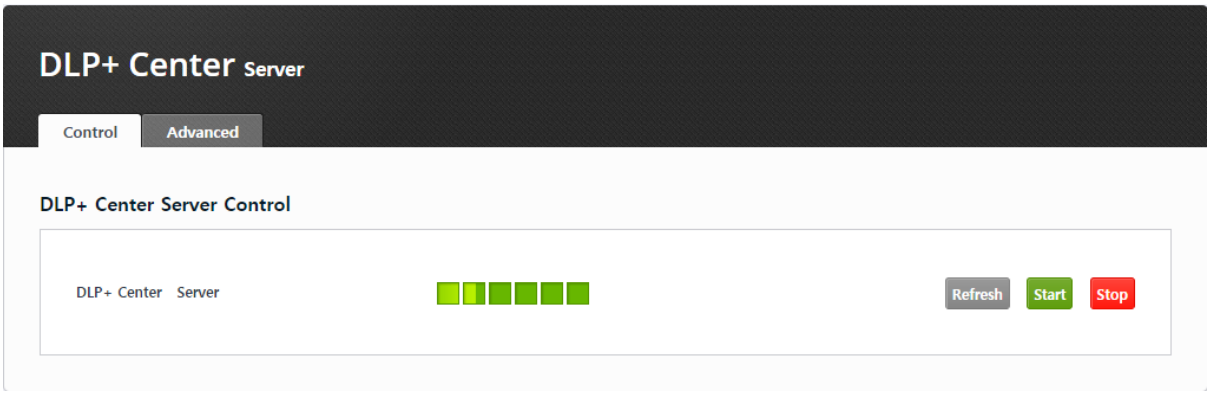
(FIGURE 3-16) VIEW AGENT UPDATE HISTORY SCREEN

SOMANSA Copyright©2015 SOMANSA All rights reserved

3.6 DLP+ Center Settings

3.6.1 Server Management

The status of the DLP+ Center Server and its operation can be set. As shown in (Figure 3-17), Restart, Start and Stop functions for the DLP+ Center Server are provided.

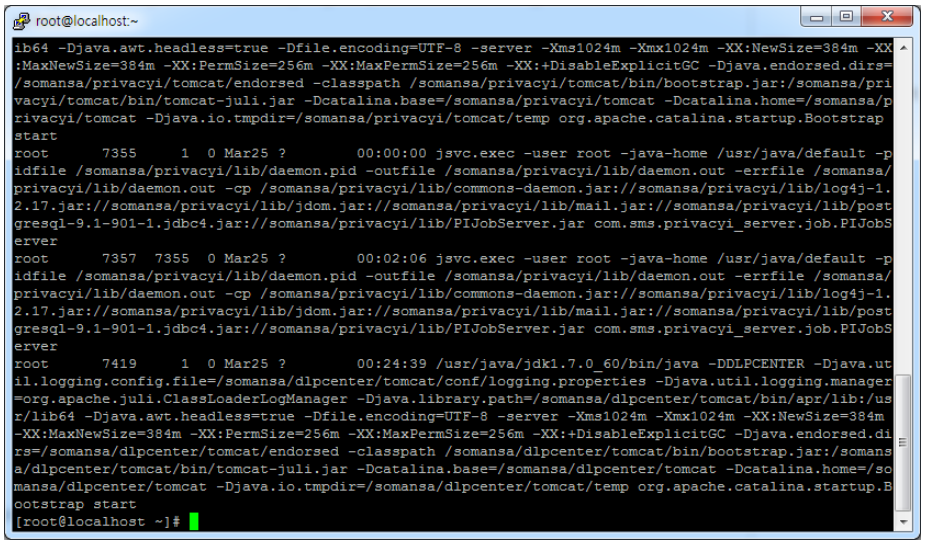


(FIGURE 3-17) DLP+CENTER SERVER MANAGEMENT SCREEN

✓ How to reconfirm service from the system console after running all services

Information about the daemon process where components (Privacy-i Server, DLP+Center, Configuration Manager, Job Server, Privacy-i Agent Update Server) are running can be viewed as below.

ps –ef | grep java


root@localhost:~
ib64 -Djava.awt.headless=true -Dfile.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:NewSize=384m -XX
:MaxNewSize=384m -XX:PermSize=256m -XX:MaxPermSize=256m -XX:+DisableExplicitGC -Djava.endorsed.dirs=
/somansa/privacyi/tomcat/endorsed -classpath /somansa/privacyi/tomcat/bin/bootstrap.jar:/somansa/pri
vacyi/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/somansa/privacyi/tomcat -Dcatalina.home=/somansa/p
rivacyi/tomcat -Djava.io.tmpdir=/somansa/privacyi/tomcat/temp org.apache.catalina.startup.Bootstrap
start
root 7355 1 0 Mar25 ? 00:00:00 jsvc.exec -user root -java-home /usr/java/default -p
idfile /somansa/privacyi/lib/daemon.pid -outfile /somansa/privacyi/lib/daemon.out -errfile /somansa/
privacyi/lib/daemon.out -cp /somansa/privacyi/lib/commons-daemon.jar://somansa/privacyi/lib/log4j-1.
2.17.jar://somansa/privacyi/lib/jdom.jar://somansa/privacyi/lib/mail.jar://somansa/privacyi/lib/post
gresql-9.1-901-1.jdbc4.jar://somansa/privacyi/lib/PIJobServer.jar com.sms.privacyi_server.job.PIJobS
erver
root 7357 7355 0 Mar25 ? 00:02:06 jsvc.exec -user root -java-home /usr/java/default -p
idfile /somansa/privacyi/lib/daemon.pid -outfile /somansa/privacyi/lib/daemon.out -errfile /somansa/
privacyi/lib/daemon.out -cp /somansa/privacyi/lib/commons-daemon.jar://somansa/privacyi/lib/log4j-1.
2.17.jar://somansa/privacyi/lib/jdom.jar://somansa/privacyi/lib/mail.jar://somansa/privacyi/lib/post
gresql-9.1-901-1.jdbc4.jar://somansa/privacyi/lib/PIJobServer.jar com.sms.privacyi_server.job.PIJobS
erver
root 7419 1 0 Mar25 ? 00:24:39 /usr/java/jdk1.7.0_60/bin/java -DDLPCENTER -Djava.ut
il.logging.config.file=/somansa/dlpcenter/tomcat/conf/logging.properties -Djava.util.logging.manager
=org.apache.juli.ClassLoaderLogManager -Djava.library.path=/somansa/dlpcenter/tomcat/bin/apr/lib:/us
r/lib64 -Djava.awt.headless=true -Dfile.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:NewSize=384m
-XX:MaxNewSize=384m -XX:PermSize=256m -XX:MaxPermSize=256m -XX:+DisableExplicitGC -Djava.endorsed.di
rs=/somansa/dlpcenter/tomcat/endorsed -classpath /somansa/dlpcenter/tomcat/bin/bootstrap.jar:/somans
a/dlpcenter/tomcat/bin/tomcat-juli.jar -Dcatalina.base=/somansa/dlpcenter/tomcat -Dcatalina.home=/so
mansa/dlpcenter/tomcat -Djava.io.tmpdir=/somansa/dlpcenter/tomcat/temp org.apache.catalina.startup.B
ootstrap start
[root@localhost ~]#

(FIGURE 3-18) JAVA SERVICE CONFIRMATION SCREEN

The status of the Apache server can be viewed as shown in the figure below for components to communicate externally.

SOMANSA Copyright©2015 SOMANSA All rights reserved

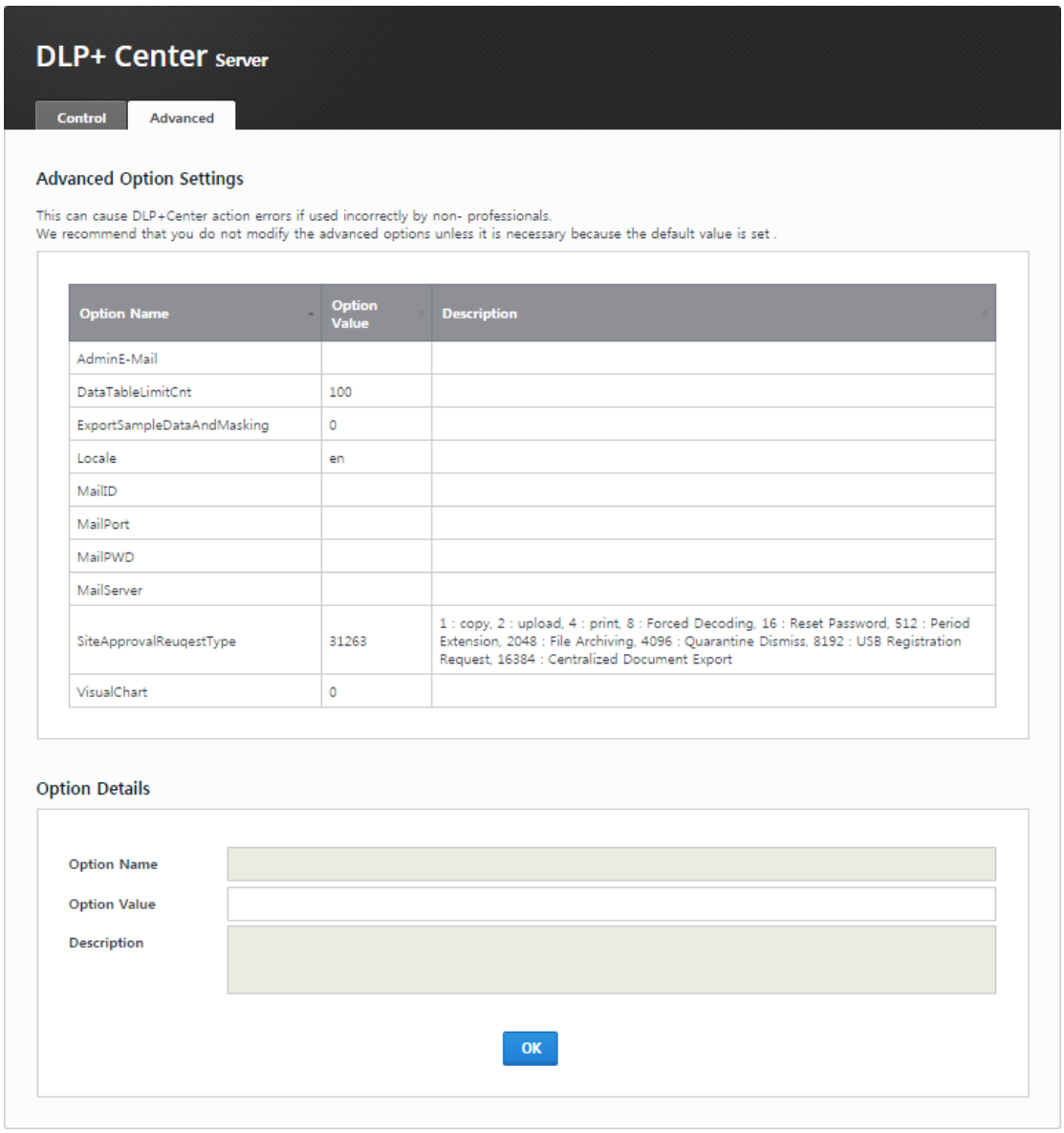
ps –ef | grep httpd (Check Apache server)

```
[root@piserver1 ~]# ps -ef | grep httpd
root      6968  6941  0 20:51 pts/2    00:00:00 grep httpd
root      7046     1  0 Oct16 ?        00:01:25 /somansa/common/httpd/bin/httpd -k start
daemon    7047  7046  0 Oct16 ?        00:23:27 /somansa/common/httpd/bin/httpd -k start
daemon    7048  7046  0 Oct16 ?        00:21:13 /somansa/common/httpd/bin/httpd -k start
daemon    7049  7046  0 Oct16 ?        00:31:32 /somansa/common/httpd/bin/httpd -k start
daemon    7131  7046  0 Oct16 ?        00:19:02 /somansa/common/httpd/bin/httpd -k start
```

(FIGURE 3-19) APACHE SERVICE CONFIRMATION SCREEN

3.6.2 Advanced Options

Options for operating DLP+ Center can be selected.



(FIGURE 3-20) DLP+CENTER ADVANCED OPTIONS

The options are provided by the DLP+ Center. However, the advanced functions can lead to errors

SOMANSA Copyright©2015 SOMANSA All rights reserved

in the DLP+ Center operation when used incorrectly by a non-experienced user. We recommend not modifying Advanced Options unless modification is absolutely necessary since default values are set. Please contact the Somansa Support Team if option changes must be checked. For the definitions of each option, please refer to the table below.

[TABLE 3-6] DEFINITION OF ADVANCED OPTIONS

Option Name	Definition
VisualChart	Whether to display chart in a report or not (0/1)
Locale	Internationalization Locale Settings (ko/en)
DataTableLimitCnt	Number of table outputs (default 100)
AdmnE-mail	Security Admin E-mail address
MailServer	SMTP Mail Server address
MailPWD	SMTP Mail Server password
MailID	SMTP Mail Server ID
MailPort	SMTP Mail Server port
ExportSampleDataMasking	Options when Exporting Incidents to Excel 0 - Exclude sample data (only including name and number of patterns), 1 - Include sample data + Masking, 2 - Include sample data (Plaintext)

☞ Effective Input Field Range

[TABLE 3-7] EFFECTIVE INPUT FIELD RANGE FOR ADVANCED OPTIONS

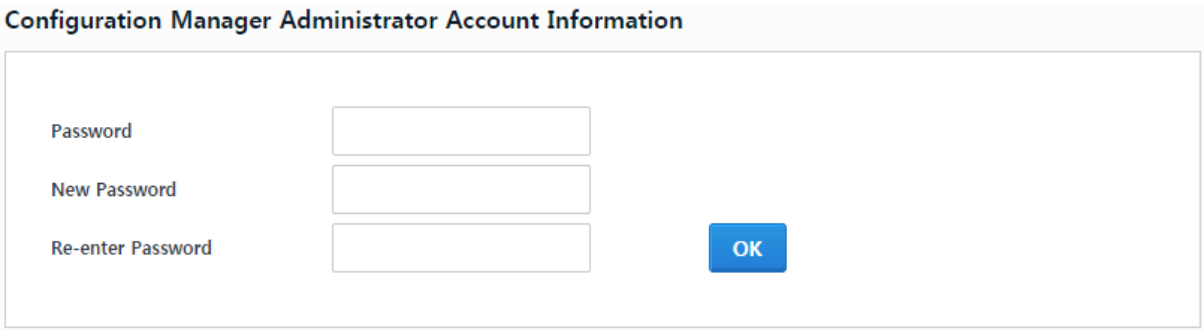
Item	Effective Range	Character	Failure Message
Option Value	0~50	Numbers	Select an option.

SOMANSA Copyright©2015 SOMANSA All rights reserved

3.7 Preferences

3.7.1 Configuration Manager Administrator Account Information

Password for the Security Admin can be changed. To change the password, enter the current password, a new password and new password confirmation. We recommend changing passwords regularly for security purposes.



(FIGURE 3-21) CONFIGURATION MANAGER ADMINISTRATOR ACCOUNT INFORMATION

☞ Effective Input Field Range

[TABLE 3-8] EFFECTIVE INPUT FIELD RANGE FOR CONTROL PANEL ADMIN ACCOUNT INFORMATION

Item	Effective Range	Character	Failure Message
Password	9~12	Numbers, uppercase/ lowercase letters, special characters	Enter the password for the current admin account.
New Password	9~12	Numbers, uppercase/ lowercase letters, special characters	Enter the new password for the admin account.
Re-enter Password	9~12	Numbers, uppercase/ lowercase letters, special characters	Enter the new password for the admin account again.

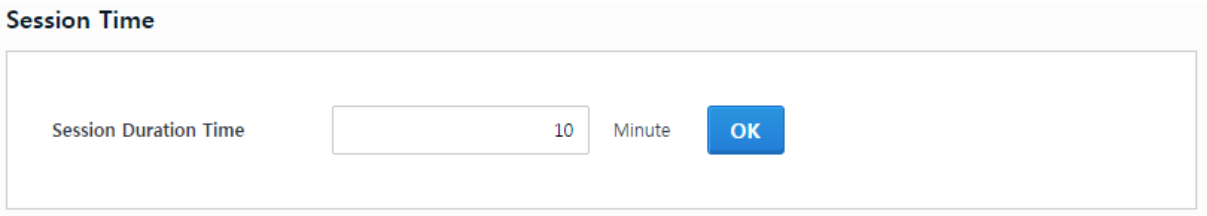
Recommendations

✓ Password should have at least 9 characters and include English letters, numbers and special characters.

SOMANSA Copyright©2015 SOMANSA All rights reserved

3.7.2 Session Time

Set the Session Duration of the Configuration Manager.



(FIGURE 3-22) SESSION TIME

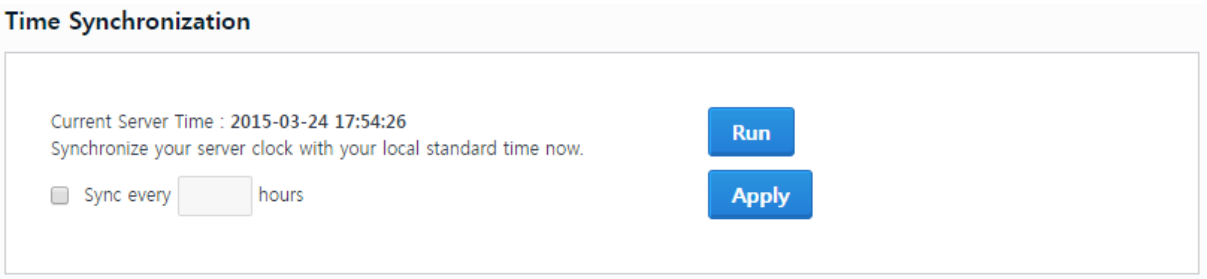
☞ Effective Input Field Range

[TABLE 3-9] EFFECTIVE INPUT FIELD RANGE FOR SESSION TIME SETTINGS

Item	Effective Range	Character	Failure Message
Session Duration	1~10	Numbers	Enter the session duration.

3.7.3 Time Synchronization

Synchronizes the time between product modules in standard time based on the NTP Server.



(FIGURE 3-23) TIME SYNCHRONIZATION

☞ Effective Input Field Range

[TABLE 3-10] EFFECTIVE INPUT FIELD RANGE FOR TIME SYNCHRONIZATION

Item	Effective Range	Character	Failure Message
Synchronization Cycle	1~99	Numbers	Enter a synchronization cycle.

SOMANSA Copyright©2015 SOMANSA All rights reserved

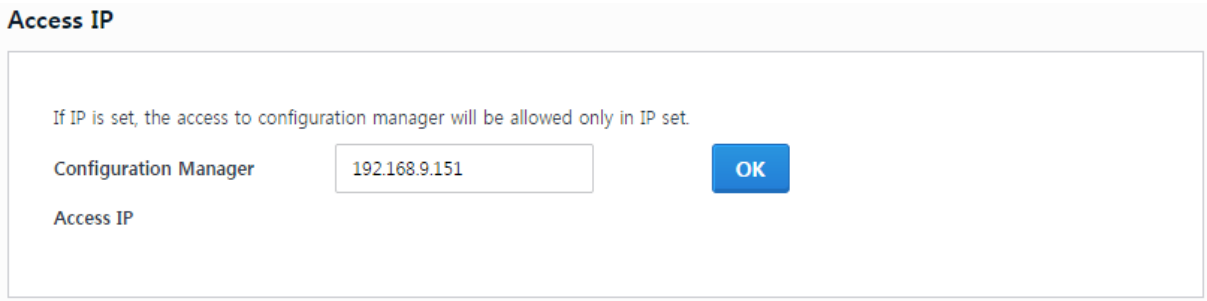
3.7.4 UID

The server UID information can be viewed for license issuance.

(FIGURE 3-24) UID

3.7.5 Access IP

Configures Access IP to the Control Panel. The Control Panel can be connected from a total of 2 IPs, including a local IP and a set IP.


Access IP
If IP is set, the access to configuration manager will be allowed only in IP set.
Configuration Manager
192.168.9.151
OK
Access IP

(FIGURE 3-25) ACCESS IP

☞ Effective Input Field Range

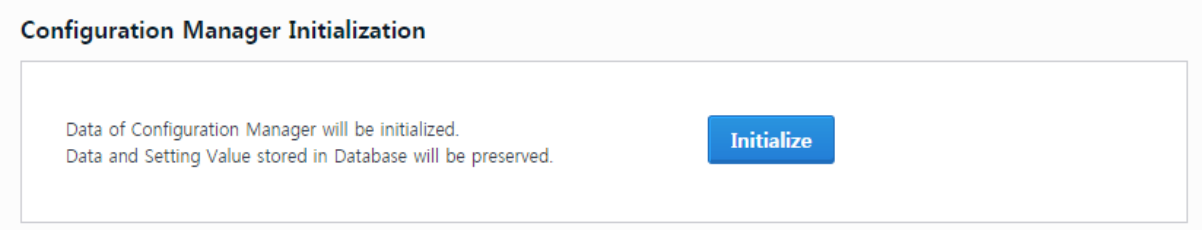
[TABLE 3-11] EFFECTIVE INPUT FIELD RANGE FOR ACCESS IP SETTINGS

Item	Effective Range	Character	Failure Message
Control Panel Access IP	15	Numbers, special characters (.)	Enter the Control Panel Access IP.

3.7.6 Configuration Manager Initialization

Initializes Control Panel settings. Initializes the product setting information and returns to status after installation. Data and setting value that are stored in the database will be preserved.

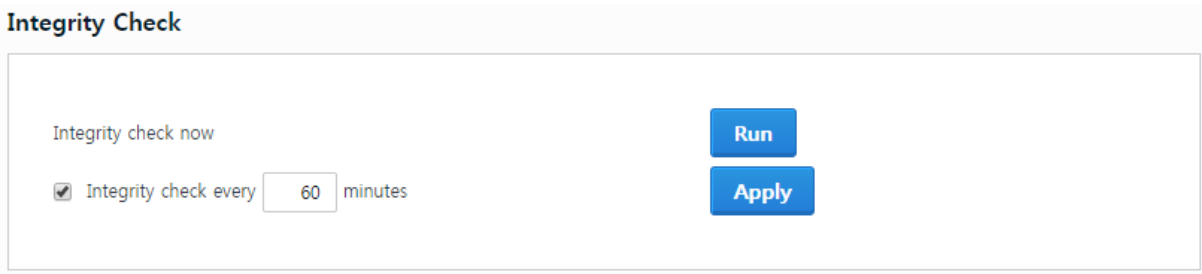
SOMANSA Copyright©2015 SOMANSA All rights reserved


Configuration Manager Initialization
Data of Configuration Manager will be initialized.
Data and Setting Value stored in Database will be preserved.
Initialize

(FIGURE 3-26) CONFIGUTAION MANAGER INITIALIZATION

3.7.7 Integrity Check

Sets the Integrity function of the product. The Integrity Inspection provides two methods, which include running a scheduled task, and a Security Admin clicking the "Run" button. This function is not activated by default, but can be used after checking 'Integrity Cycle'.



(FIGURE 3-27) INTEGRITY CHECK

☞ Effective Input Field Range

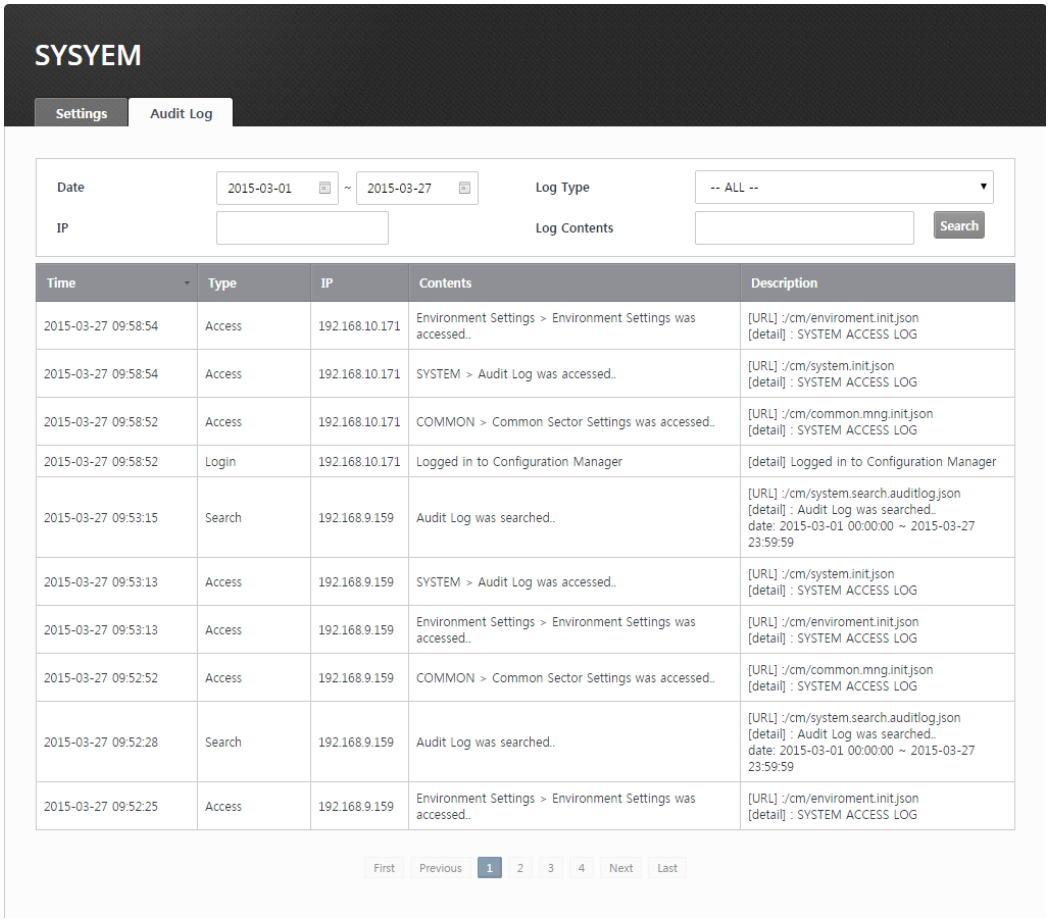
[TABLE 3-12] EFFECTIVE INPUT FIELD RANGE FOR INTEGRITY FUNCTION SETTINGS

Item	Effective Range	Character	Failure Message
Integrity Cycle	99	Numbers	Enter the integrity function cycle.

3.8 SYSTEM Audit Logs

This screen shows Audit Logs of the SYSTEM. All events of the Security Admin from the initial installation to operation are saved. In addition, Audit Logs can be viewed by setting the desired time period. The Audit Logs are displayed by categorizing Date, Type, IP, Content and Description.

SOMANSA Copyright©2015 SOMANSA All rights reserved

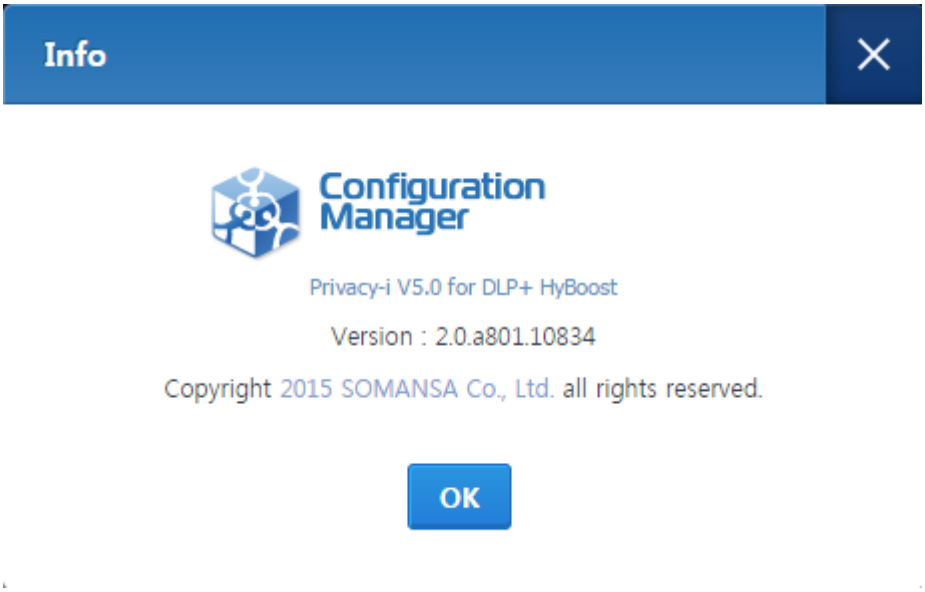


(FIGURE 3-28) VIEW SYSTEM AUDIT LOGS

3.9 Check Privacy-i Version

The version of the Configuration Manager can be checked on this screen. Click the button at the top right to check the version.

SOMANSA Copyright©2015 SOMANSA All rights reserved

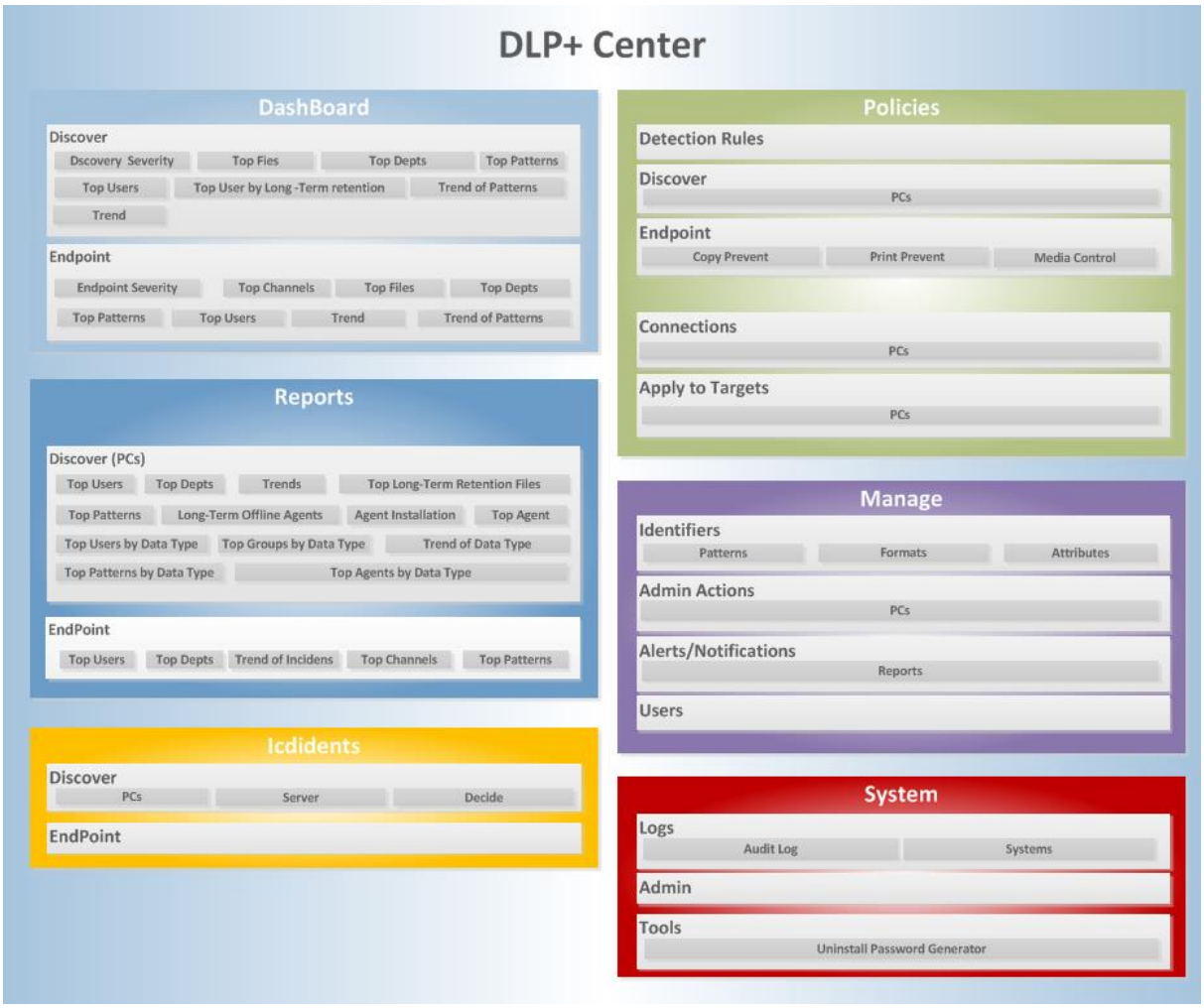


(FIGURE 3-29) CHECK CONFIGURATION MANAGER VERSION

SOMANSA Copyright©2015 SOMANSA All rights reserved

4. DLP+ Center

Privacy-i is a product that provides Data Protection and Host Data Loss Prevention by searching and identifying personal and confidential data stored on a company PC and provides technological and managerial protection measures such as deletion. In addition, Privacy-i provides an Endpoint Data Loss Prevention solution, which controls dataflow from a user PC to an external channel. Privacy-i is operated and managed by the DLP+ Center, a central management console. Since the DLP+ Center is operated as a web server, the authorized admin can connect to the DLP+ Center through the company intranet anytime and anywhere for a convenient operating environment.

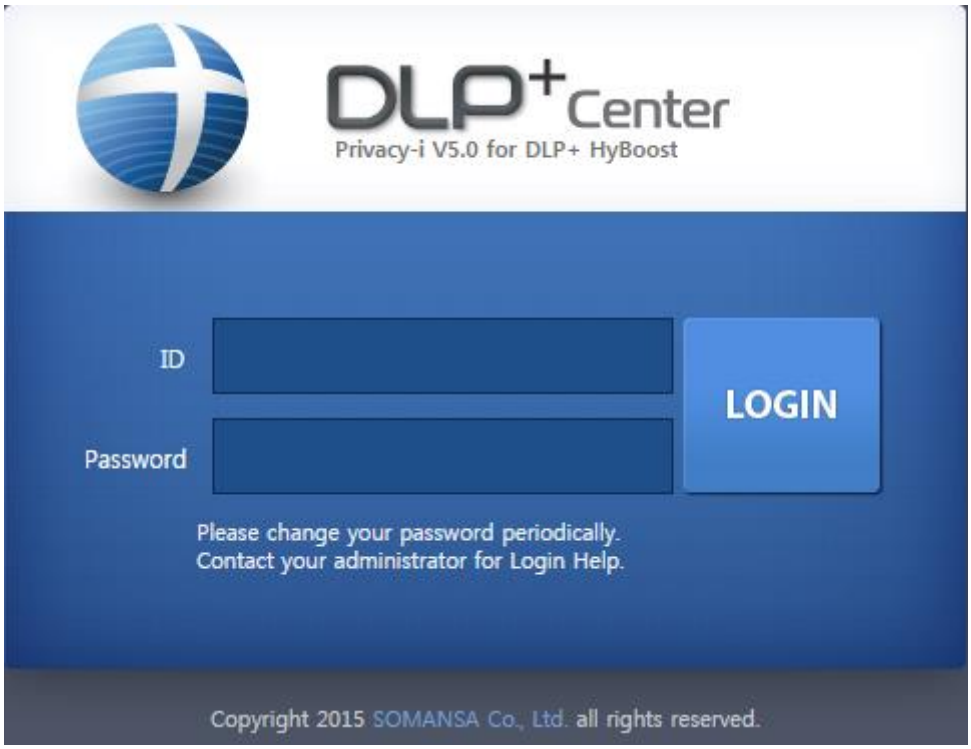


(FIGURE 4-1) FUNCTIONS PROVIDED BY THE DLP+ CENTER

The DLP+ Center is categorized into Dashboard, Report, Policy, Incidents, Manage and System as follows (see Figure 4-1). Dashboard updates the personal information status and sensitive information dataflow in real time to allow the admin to view information on the main issues.

SOMANSA Copyright©2015 SOMANSA All rights reserved

Report provides a variety of reports for each condition through the detected logs in a PC. Policy allows for the management of the confidential data inspection policy that is specified to a user PC. In addition, Incidents provide information on detected confidential data and allowed/blocked log in detail. In Manage, the additional functions for the server and agent can be set. Through System, the Audit Logs, Event and Account Authorization Settings of the DLP+ Center admin can be viewed.



(FIGURE 4-2) DLP+ CENTER LOGIN SCREEN

When the DLP+ Center URL address is entered into a web browser, a login screen appears as shown in (Figure 4-2). When the account information set in Configuration Manager is entered, the DLP+ Center can be successfully logged in. Please note that the session becomes locked if the wrong password is entered more than 3 times.

☞ Effective Input Field Range

[TABLE 4-1] EFFECTIVE INPUT FIELD RANGE UPON DLP+ CENTER LOGIN

Item	Effective Range	Character	Failure Message
ID	5~100	Letters	Enter ID.
Password	9~41	Numbers, uppercase/ lowercase letters, special	Enter password.

SOMANSA Copyright©2015 SOMANSA All rights reserved

		characters	

Recommendations

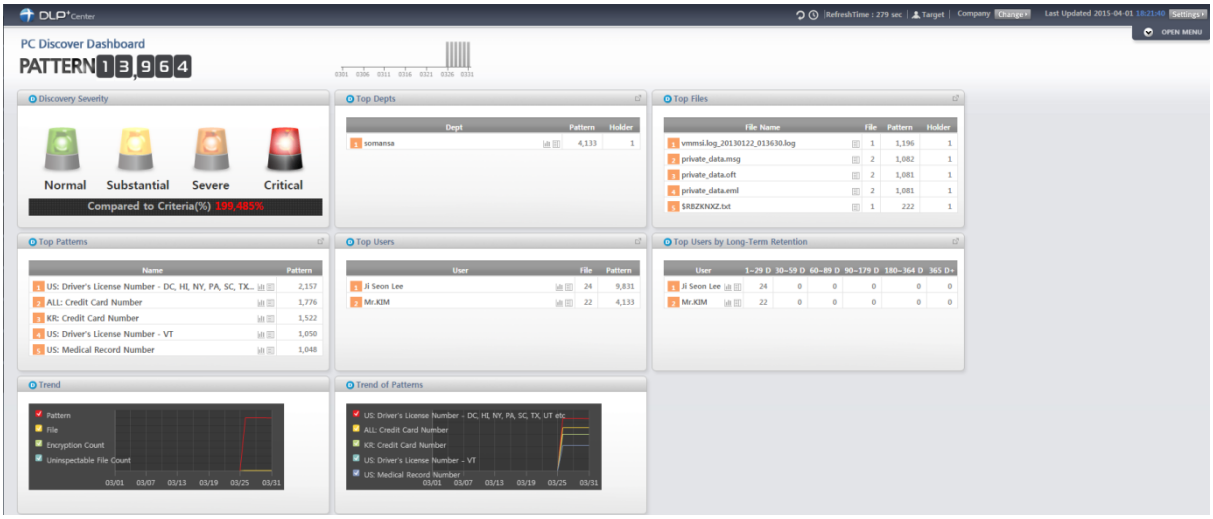
✓ Password should have at least 9 characters and include English letters, numbers and special characters.

4.1 Dashboard

Dashboard is categorized into Discover and Endpoint, and provides department or user-specific data retained, leakage path and data in real time. Such data are composed of components, and are displayed in order based on the most recent, or retained sensitive data. It has the advantage of quickly identifying the severity of retained data and retaining status by selecting the component and pattern and setting the department for intensive monitoring.

4.1.1 Discover

Discover Dashboard collects inspection information on sensitive data retained in a user PC, and provides information. Discover has 8 components, including '(D) Discovery Severity', '(D) Top Depts', '(D)Top Patterns', '(D) Top Users', '(D) Trend', '(D) Top Files', '(D) Trend of Patterns' and '(D) Top Users by Long-Term Retention'.

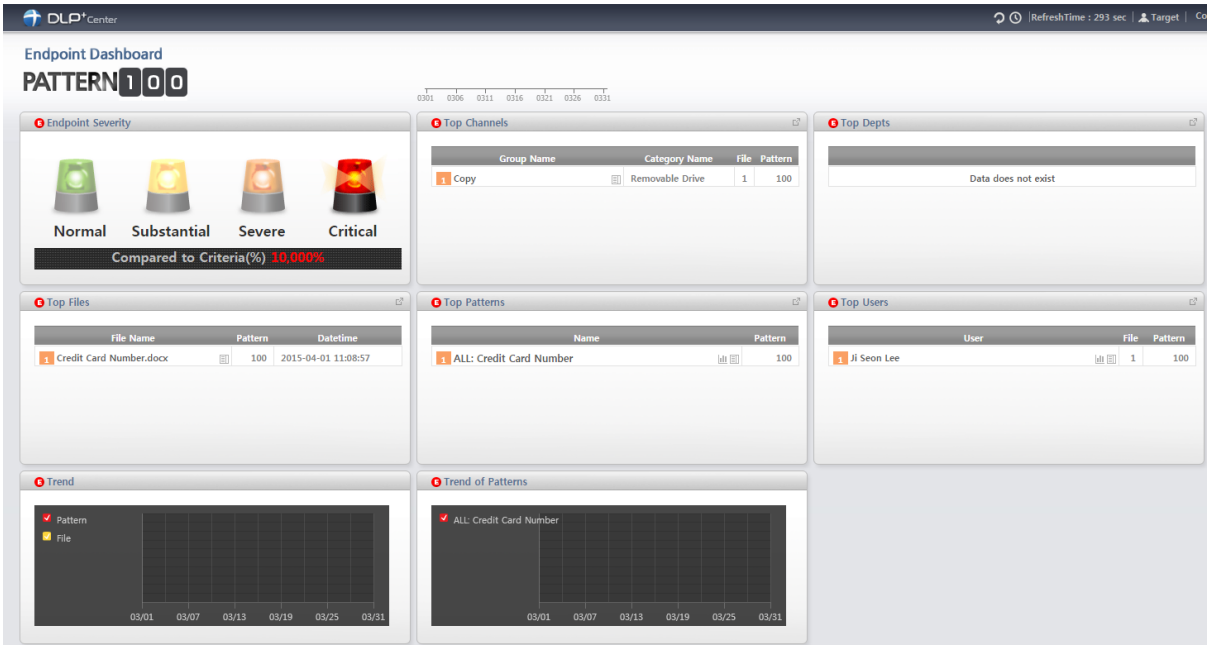


(FIGURE 4-3) DASHBOARD: DISCOVER INFORMATION

SOMANSA Copyright©2015 SOMANSA All rights reserved

4.1.2 Endpoint

Endpoint Dashboard collects inspection information on sensitive data retained in a user PC, and provides information. Discover has 8 components, including '(E) Endpoint Severity', '(E) Top Depts', '(E) Top Patterns', '(E) Top Users', '(E) Trend', '(E) Top Files', and '(E) Top Channels' .

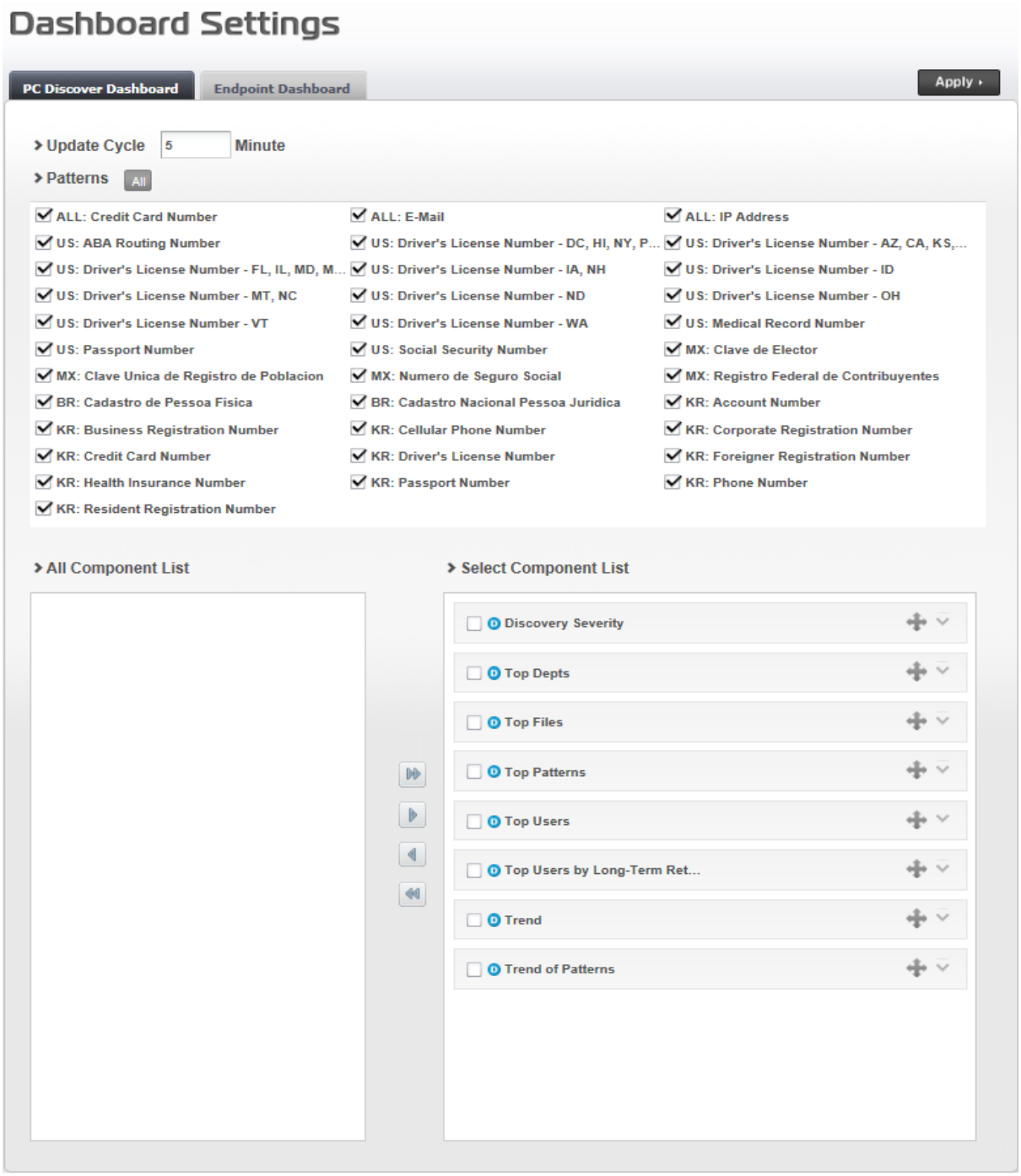


(FIGURE 4-4) DASHBOARD: ENDPOINT INFORMATION

SOMANSA Copyright©2015 SOMANSA All rights reserved

4.1.3 Settings

(Figure 4-5) is the Preferences screen where Dashboard data information can be configured. The options that can be selected in the Settings are Select Component, Select Pattern to be used for each component, and Renewal Cycle and displays the data applied to the Dashboard according to this set value.



(FIGURE 4-5) DASHBOARD: SETTINGS

SOMANSA Copyright©2015 SOMANSA All rights reserved

4.2 Reports

Reports run the analysis results by condition about confidential data retained (Discover) in a user PC within the network and the exported/ blocked log of Endpoint. Since Reports display a variety of graphs, lists and main result items of the detected results, the Admin has the advantage of being able to quickly analyze according to the selected criteria.

[TABLE 4-2] REPORT PROVIDED BY DLP+ CENTER

		Type	Content
Discover	PC	Top Users	Displays data by top users in order who retain the most confidential data based on the selected department.
		Top Agent	Displays the ranking of confidential data files retained by an agent.
		Top Depts	Displays data by top departments in order that retain the most confidential data based on the selected department.
		Trends	Displays results for confidential data retained in a user PC regarding inspected date log.
		Top Long-Term Retention Files	Displays data by top PCs which retain confidential data files for a long time.
		Top Patterns	Displays data by top patterns that retain confidential data regarding a selected department or user.
		Long-Term Offline Agents	Searches agents which were offline for a long time
		Agent Installations	Identifies Privacy-i installation status of users.
		Top Users by Data Type	Checks data 'Categorization (%)' and 'Categorization Content' in order by a 'user'.
		Top Depts by Data Type	Checks data 'Categorization (%)' and 'Categorization Content' in order by a 'Dept'.
		Trend of Data Type	Checks variation by date for data patterns and files.
		Top Patterns by Data Type	Checks 'Total Number of Patterns' and 'Categorization (%)' by data type.
		Top Agents by Data Type	Checks the data categorization ranking by an agent.

SOMANSA Copyright©2015 SOMANSA All rights reserved

Endpoint	Top Users	Displays data by top users who have the most exports/blocks in order.
	Top Depts	Displays data by top departments that have the most exports/blocks
	Trends	Displays trend results of exported/blocked logs based on the selected department/user.
	Top Channels	Displays data by top channels which have the most exports/blocks
	Top Patterns	Displays data by top patterns which have the most exports/blocks

SOMANSA Copyright©2015 SOMANSA All rights reserved

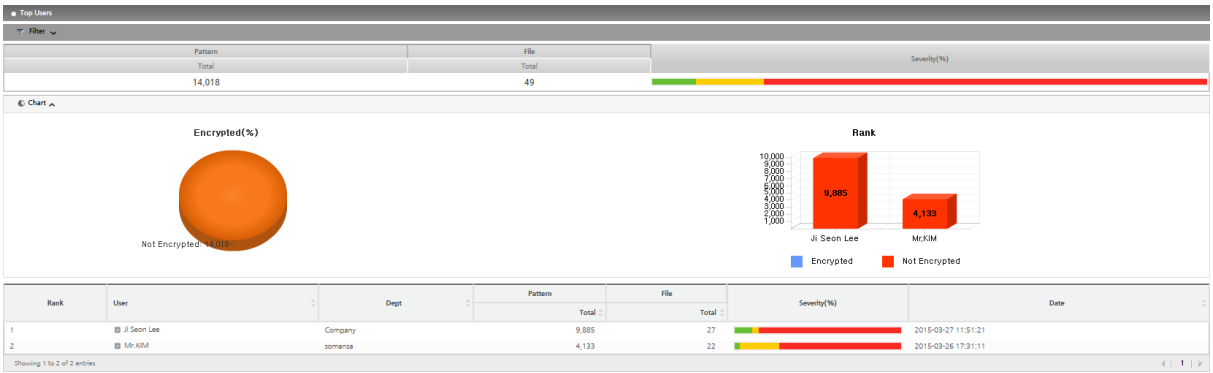
4.2.1 Discovery

4.2.1.1 PC

By using the results of retained confidential data inspection on a PC, Reports include 'Top Users', 'Top Depts', 'Trend', 'Top Users by Long Term Retention' and 'Top Patterns' based on the detected number of confidential data patterns or files for a specific department · user, and 'Long Term Offline Agents', 'Agent Distribution' for the agent status.

- Top Users

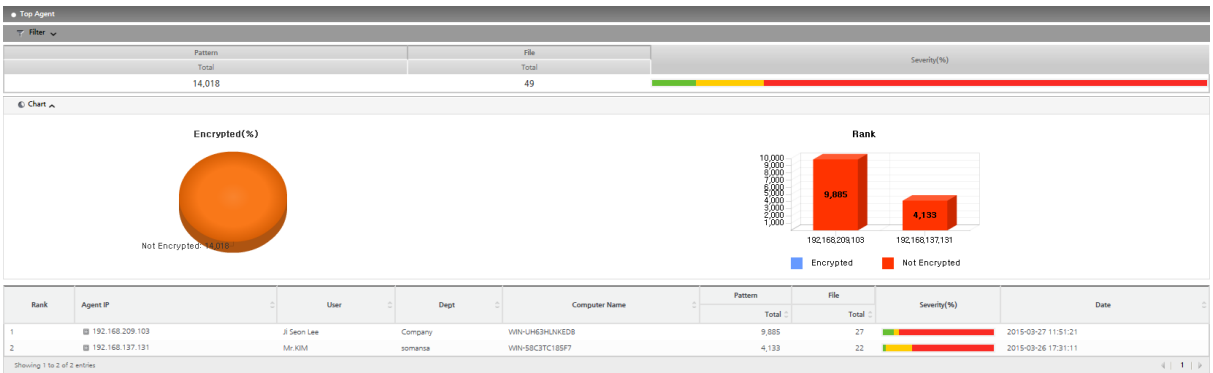
Displays the top users who retain the most confidential data files detected from a user PC in order and the number of detections. The list of top users who retain the most confidential data by selected department is displayed at the bottom.



(FIGURE 4-6) REPORT-PC: RESULTS FOR TOP USERS

- Top Agents

Displays the top severity (%) of confidential data detected from a user PC in order and the top list of detected severity results based on a user IP.

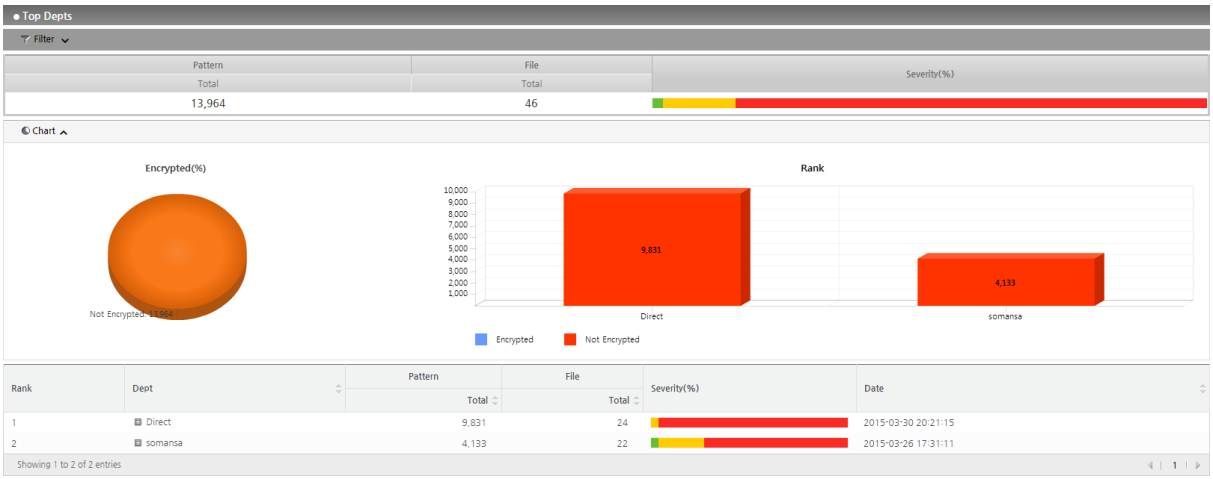


(FIGURE 4-7) REPORT-PC: RESULTS FOR TOP AGENTS

SOMANSA Copyright©2015 SOMANSA All rights reserved

- Top Depts

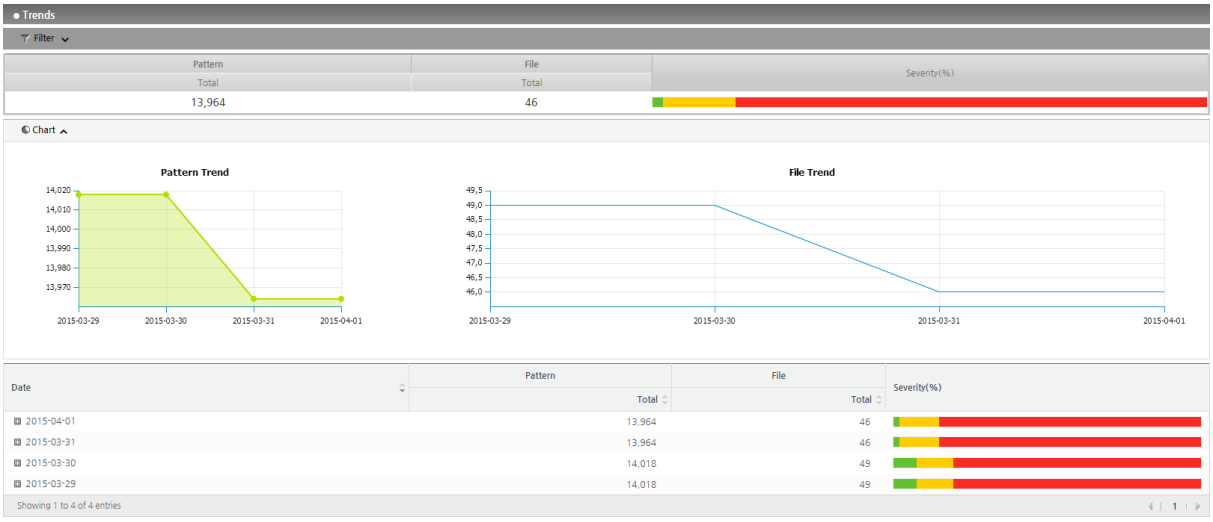
Displays data based on a "Dept".



(FIGURE 4-8) REPORT-PC: RESULTS FOR TOP DEPTS

- Trends

Displays the patterns trends of departments and users that retain confidential data files, severity (%) and. indicates confidential data which has been retained per period.

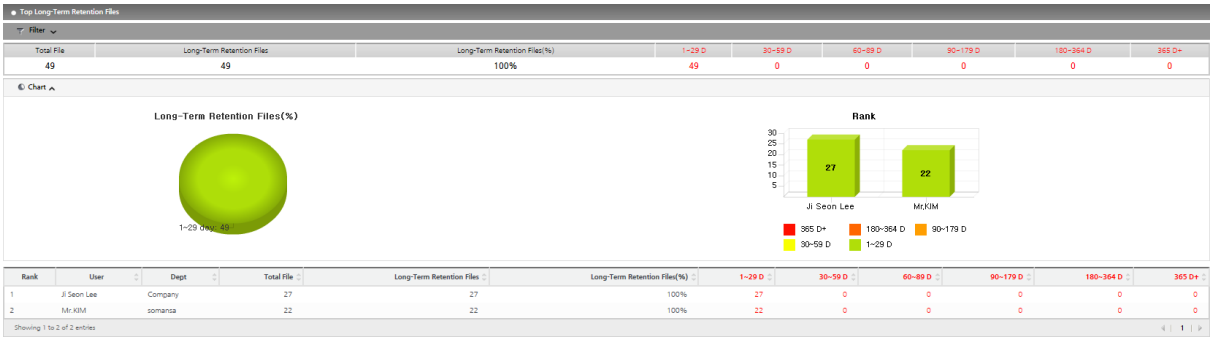


(FIGURE 4-9) REPORT-PC: RESULTS FOR TREND

- Top Long Term Retention Files

Displays data for files which include confidential data for an extended period of time. The retention period of a detected file and saved confidential data (customer information, personal usage) can be checked.

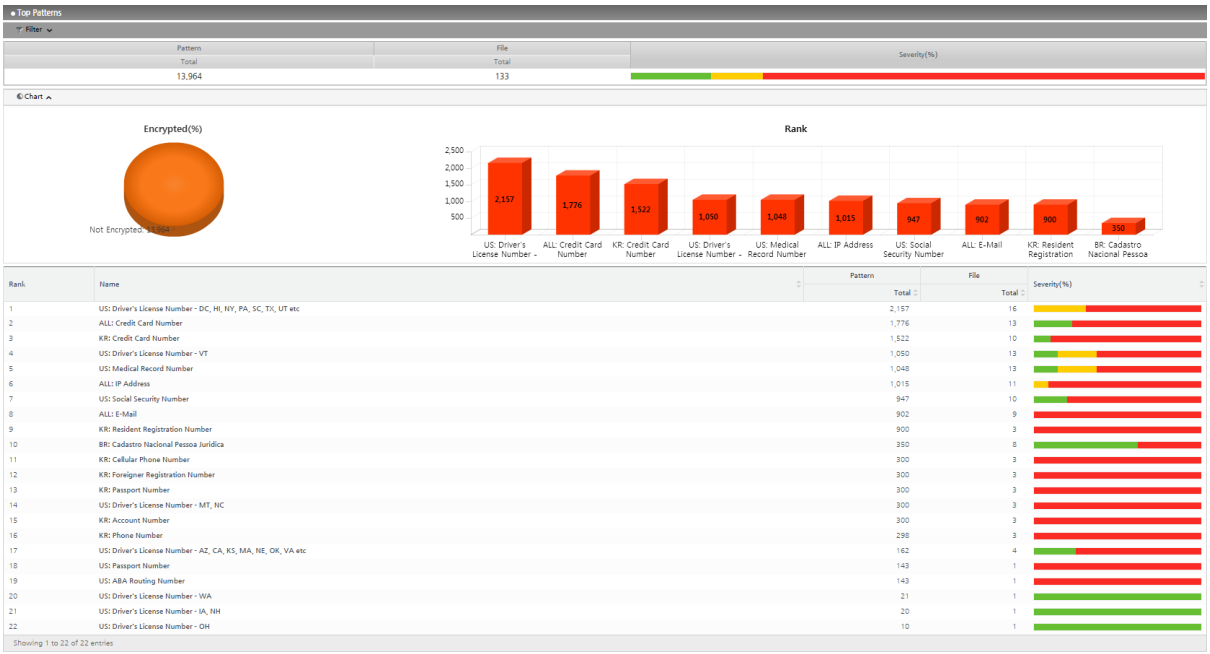
SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 4-10) REPORT-PC: RESULTS FOR TOP USERS BY LONG TERM RETENTION

- Top Patterns

Displays data based on a "pattern"..

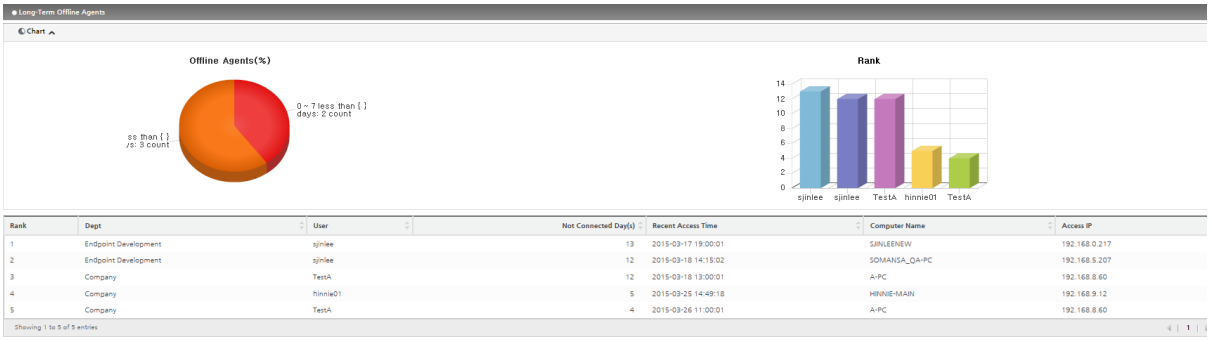

Top Patterns
Filter
Pattern
File
Severity(%)
Total
Total
13,964
133
Chart
Encrypted(%)
Not Encrypted
Rank
2,157
1,776
1,522
1,050
1,048
1,015
947
902
900
350
US: Driver's License Number -
ALL: Credit Card Number
KR: Credit Card Number
US: Driver's License Number -
US: Medical Record Number
ALL: IP Address
US: Social Security Number
ALL: E-Mail
KR: Resident Registration
BR: Cadastro Nacional Pessoa
Rank
Name
Pattern
File
Severity(%)
Total
Total
1 US: Driver's License Number - DC, HI, NY, PA, SC, TX, UT etc 2,157 16
2 ALL: Credit Card Number 1,776 13
3 KR: Credit Card Number 1,522 10
4 US: Driver's License Number - VT 1,050 13
5 US: Medical Record Number 1,048 13
6 ALL: IP Address 1,015 11
7 US: Social Security Number 947 10
8 ALL: E-Mail 902 9
9 KR: Resident Registration Number 900 3
10 BR: Cadastro Nacional Pessoa Jurídica 350 8
11 KR: Cellular Phone Number 300 3
12 KR: Foreigner Registration Number 300 3
13 KR: Passport Number 300 3
14 US: Driver's License Number - MT, NC 300 3
15 KR: Account Number 300 3
16 KR: Phone Number 298 3
17 US: Driver's License Number - AZ, CA, KS, MA, NE, OK, VA etc 162 4
18 US: Passport Number 143 1
19 US: ABA Routing Number 143 1
20 US: Driver's License Number - WA 21 1
21 US: Driver's License Number - IA, NH 20 1
22 US: Driver's License Number - OH 10 1
Showing 1 to 22 of 22 entries

(FIGURE 4-11) REPORT-PC: RESULTS FOR TOP PATTERNS

- Long Term Offline Agents

Displays data based on agents which were offline on the server for an extended period of time.

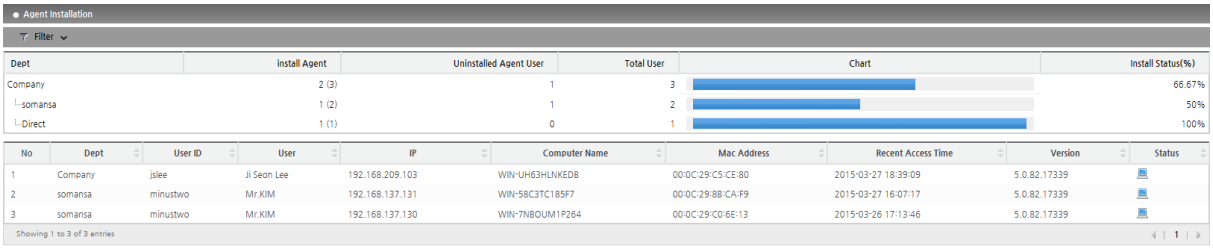
SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 4-12) REPORT-PC: RESULTS FOR LONG TERM OFFLINE AGENTS

- Agent Installations

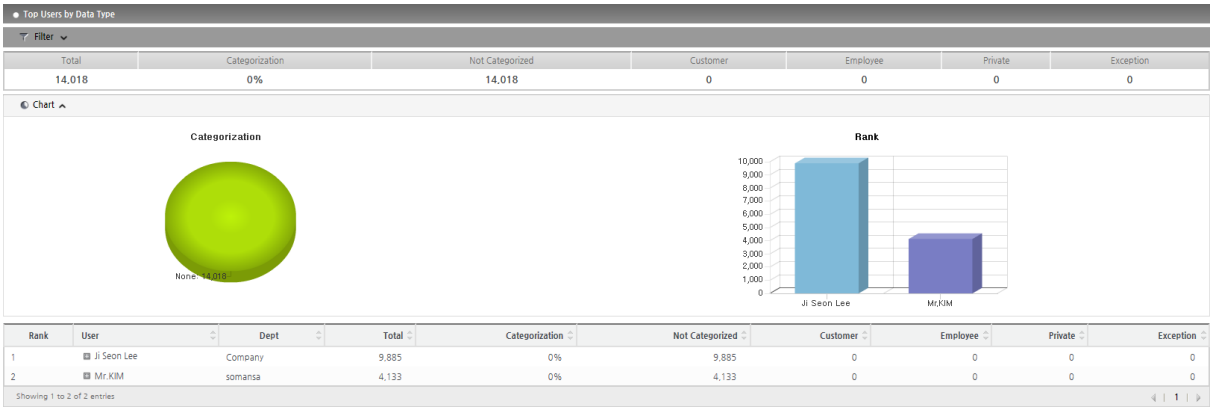
Displays user data with the agent installed based on Synchronized User Information. The agent installation status in a company can be checked in output Report.



(FIGURE 4-13) REPORT-PC: AGENT INSTALLATIONS

- Top Users by Data Type

Top data [Categorization (%)] and [Categorization Content] can be checked by a 'user'. The rankings of the Number of Patterns and Categorization (%) for Not Categorized, Customer, Employee, Personal, Business and Exception can be checked.

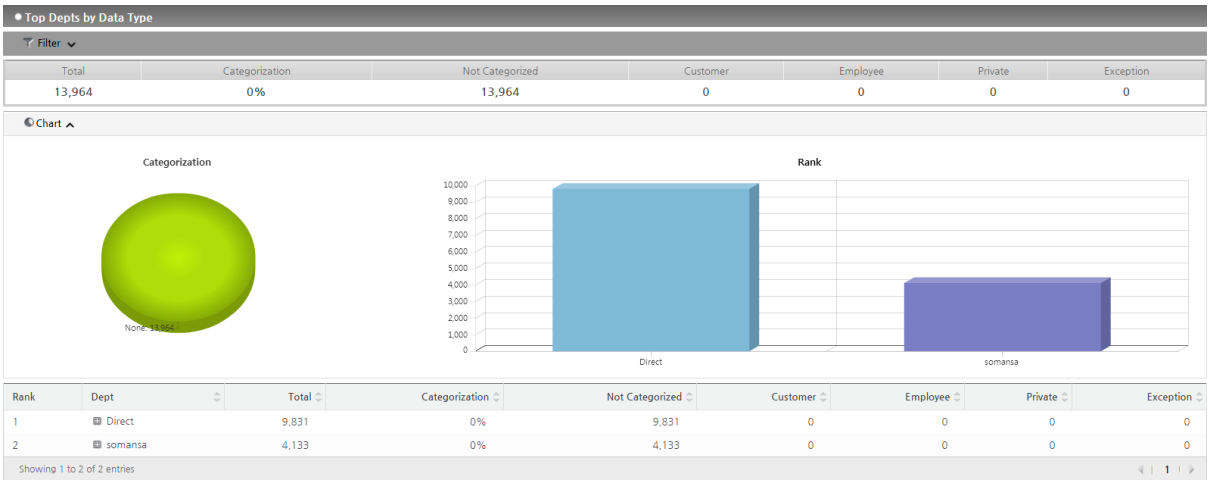


(FIGURE 4-14) REPORT-PC: TOP USERS BY DATA TYPE

SOMANSA Copyright©2015 SOMANSA All rights reserved

- Top Depts by Data Type

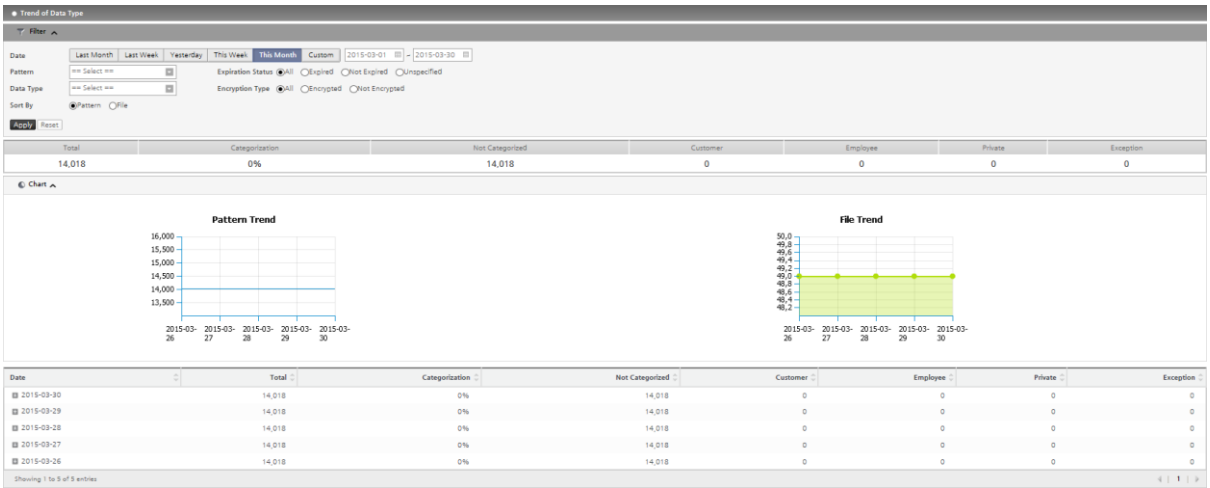
Top data [Categorization (%)] and [Categorization Content] can be checked by a 'Dept'. The rankings of the Number of Patterns and Categorization (%) for Not Categorized, Customer, Employee, Personal and Exception can be checked.



(FIGURE 4-15) REPORT-PC: TOP GROUPS BY DATA TYPE

- Trend of Data Type

Variation by date for the data pattern and file can be checked. Trends by pattern and file can be viewed in graphs and tables.

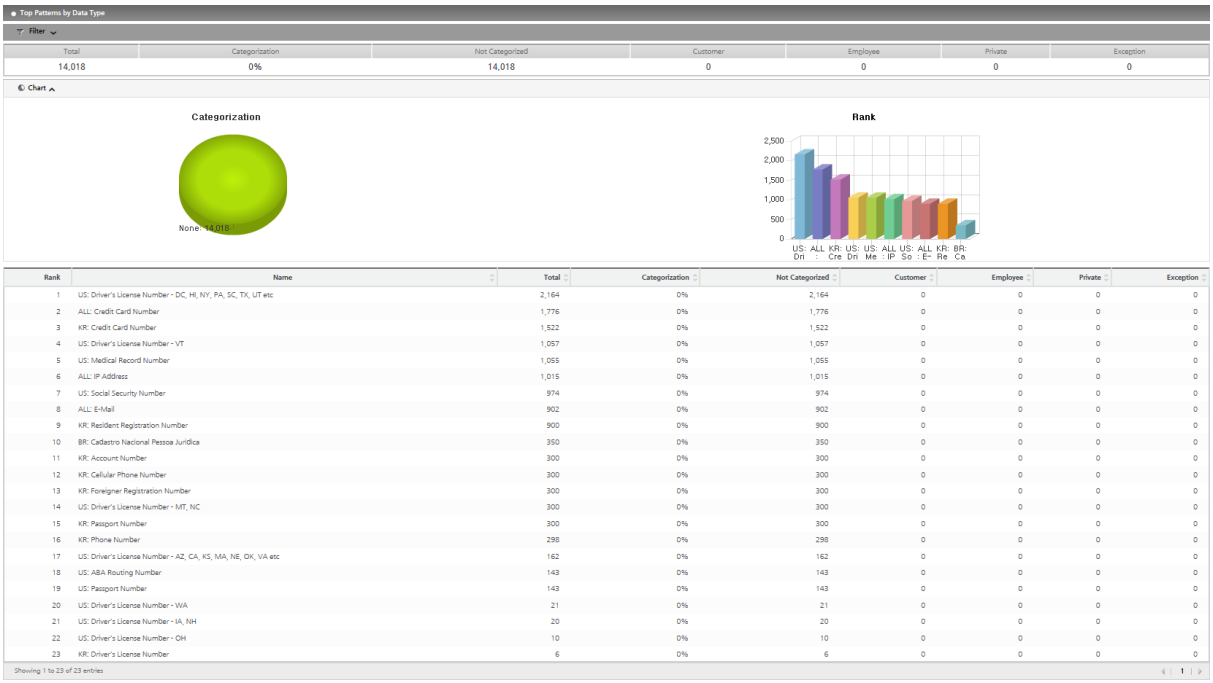


(FIGURE 4-16) REPORT-PC: TREND OF DATA TYPE

SOMANSA Copyright©2015 SOMANSA All rights reserved

- Top Patterns by Data Type

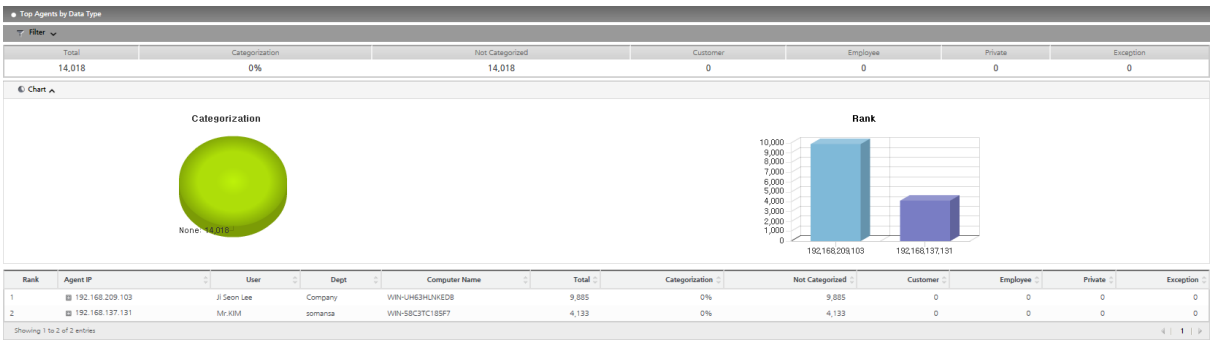
'Total Number of Patterns' and 'Categorization (%)' can be viewed by data type. The Number of Patterns and Categorization (%) for Not Categorized, Customer, Employee, and Exception can be checked by data type in order.


Top Patterns by Data Type
Filter
Total
Categorization
Not Categorized
Customer
Employee
Private
Exception
14,018
0%
14,018
0
0
0
0
Chart
Categorization
None 14,018
Rank
2,500
2,000
1,500
1,000
500
0
Rank
Name
Total
Categorization
Not Categorized
Customer
Employee
Private
Exception
1 US: Driver's License Number - DC, HI, NY, PA, SC, TX, UT etc 2,164 0% 2,164 0 0 0 0
2 ALL: Credit Card Number 1,776 0% 1,776 0 0 0 0
3 KR: Credit Card Number 1,522 0% 1,522 0 0 0 0
4 US: Driver's License Number - VT 1,057 0% 1,057 0 0 0 0
5 US: Medical Record Number 1,055 0% 1,055 0 0 0 0
6 ALL: IP Address 1,015 0% 1,015 0 0 0 0
7 US: Social Security Number 974 0% 974 0 0 0 0
8 ALL: E-Mail 902 0% 902 0 0 0 0
9 KR: Resident Registration Number 900 0% 900 0 0 0 0
10 BR: Cadastro Nacional Pessoa Jurídica 350 0% 350 0 0 0 0
11 KR: Account Number 300 0% 300 0 0 0 0
12 KR: Cellular Phone Number 300 0% 300 0 0 0 0
13 KR: Foreigner Registration Number 300 0% 300 0 0 0 0
14 US: Driver's License Number - MT, NC 300 0% 300 0 0 0 0
15 KR: Passport Number 300 0% 300 0 0 0 0
16 KR: Phone Number 298 0% 298 0 0 0 0
17 US: Driver's License Number - AZ, CA, KS, MA, NE, OK, VA etc 162 0% 162 0 0 0 0
18 US: ABA Routing Number 143 0% 143 0 0 0 0
19 US: Passport Number 143 0% 143 0 0 0 0
20 US: Driver's License Number - WA 21 0% 21 0 0 0 0
21 US: Driver's License Number - IA, NH 20 0% 20 0 0 0 0
22 US: Driver's License Number - OH 10 0% 10 0 0 0 0
23 KR: Driver's License Number 6 0% 6 0 0 0 0
Showing 1 to 23 of 23 entries
1

(FIGURE 4-17) REPORT-PC: TOP PATTERNS BY DATA TYPE

- Top Agents by Data Type

Top Agents can be viewed by data type. The Number of Patterns and Categorization (%) for Not Categorized, Customer, Employee, Personal and Exception can be checked by data type in order.



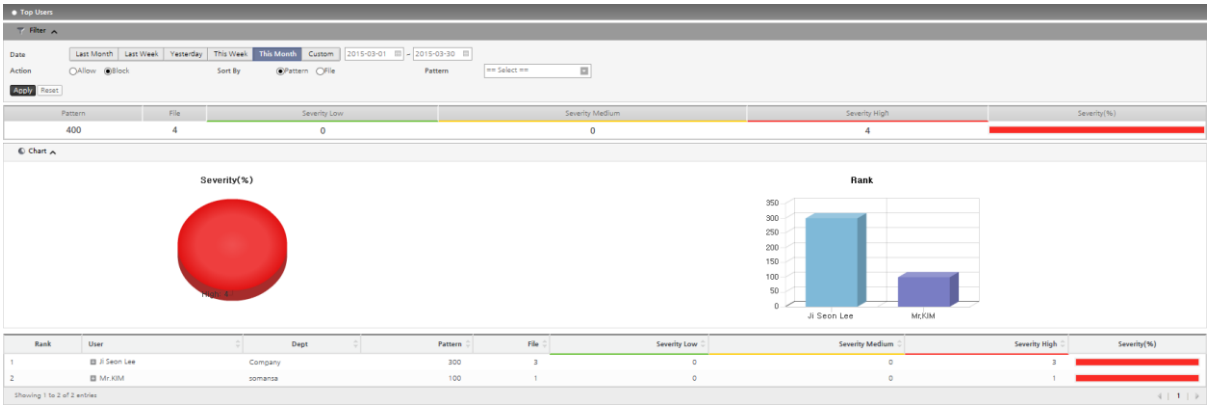
(FIGURE 4-18) REPORT-PC: TOP AGENTS BY DATA TYPE

SOMANSA Copyright©2015 SOMANSA All rights reserved

4.2.2 Endpoint

- Top Users

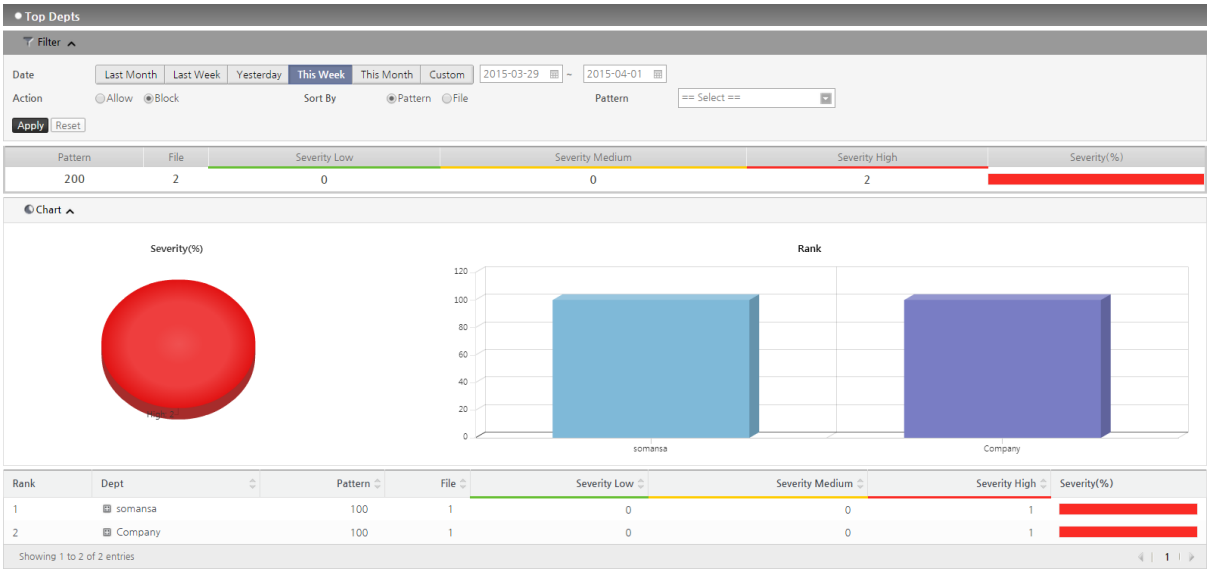
Displays data including allowed/ blocked patterns by policy, file and severity (%) by user in order. Through Report, top users who exported the most confidential data can be viewed.



(FIGURE 4-19) TOP USERS

- Top Depts

Displays data including allowed/ blocked patterns by policy, file and severity (%) by department in order. Through report, top departments which exported the most confidential data can be viewed.

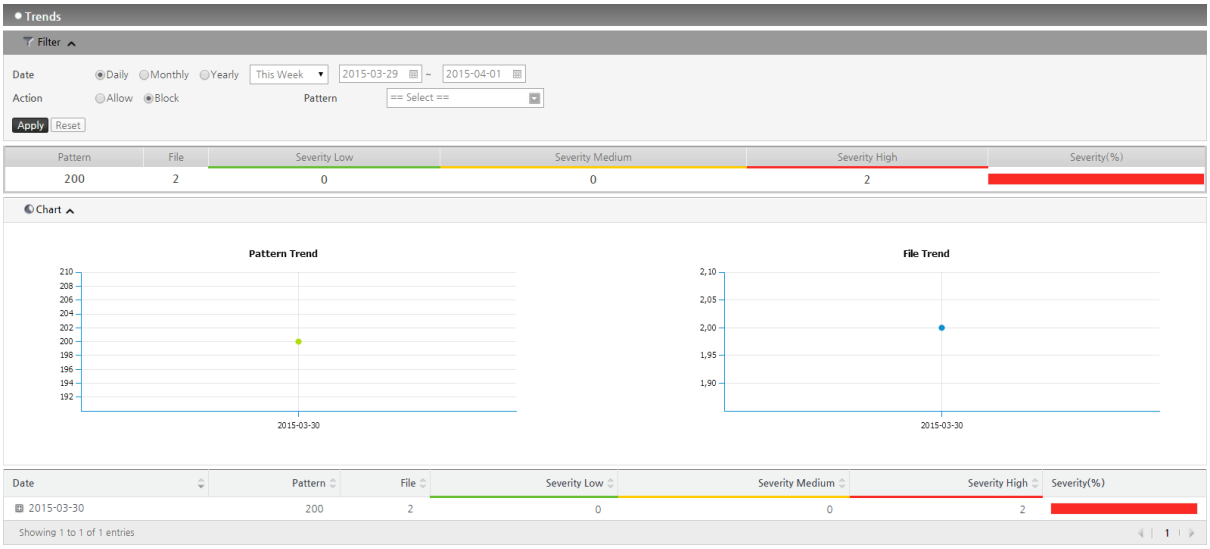


(FIGURE 4-20) TOP DEPTS

SOMANSA Copyright©2015 SOMANSA All rights reserved

- Trends

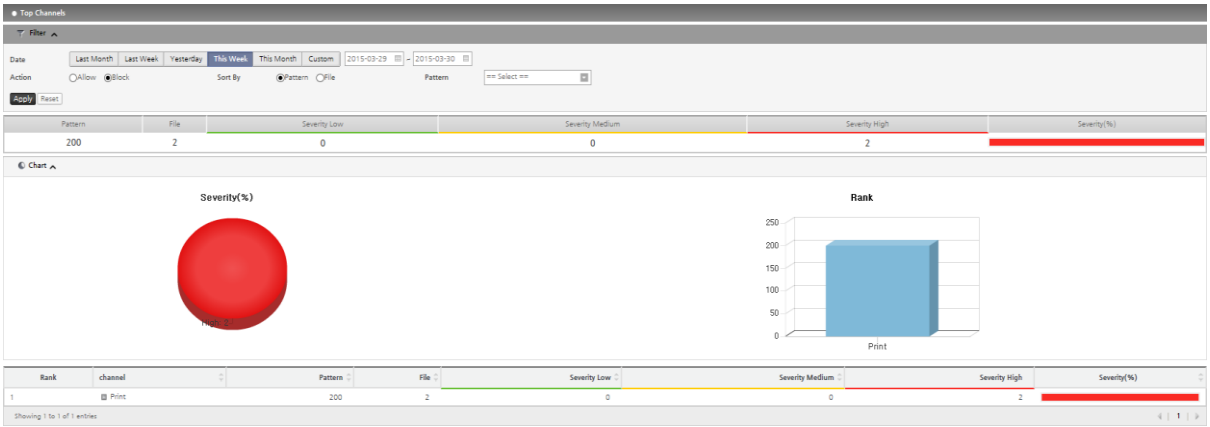
Displays trend of allowed/ blocked patterns by policy, file and severity (%) and shows the trend of departments and users which exported the most confidential data files in graphs and lists.



(FIGURE 4-21) TRENDS

- Top Channels

Displays the top channels of patterns, files and severity (%) for allowed/ blocked leakage paths.

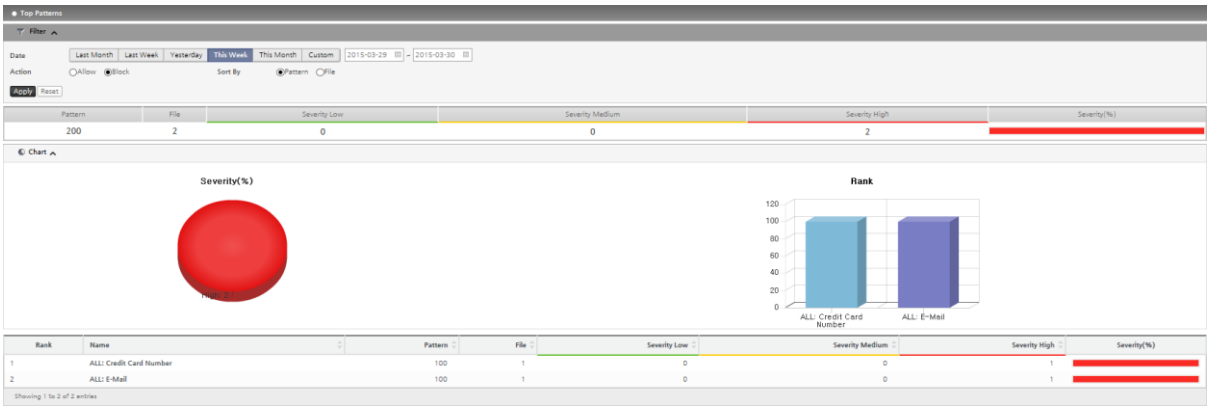


(FIGURE 4-22) TOP CHANNELS

SOMANSA Copyright©2015 SOMANSA All rights reserved

- Top Patterns

Displays the allowed/ blocked data, based on patterns.



(FIGURE 4-23) TOP PATTERNS

SOMANSA Copyright©2015 SOMANSA All rights reserved

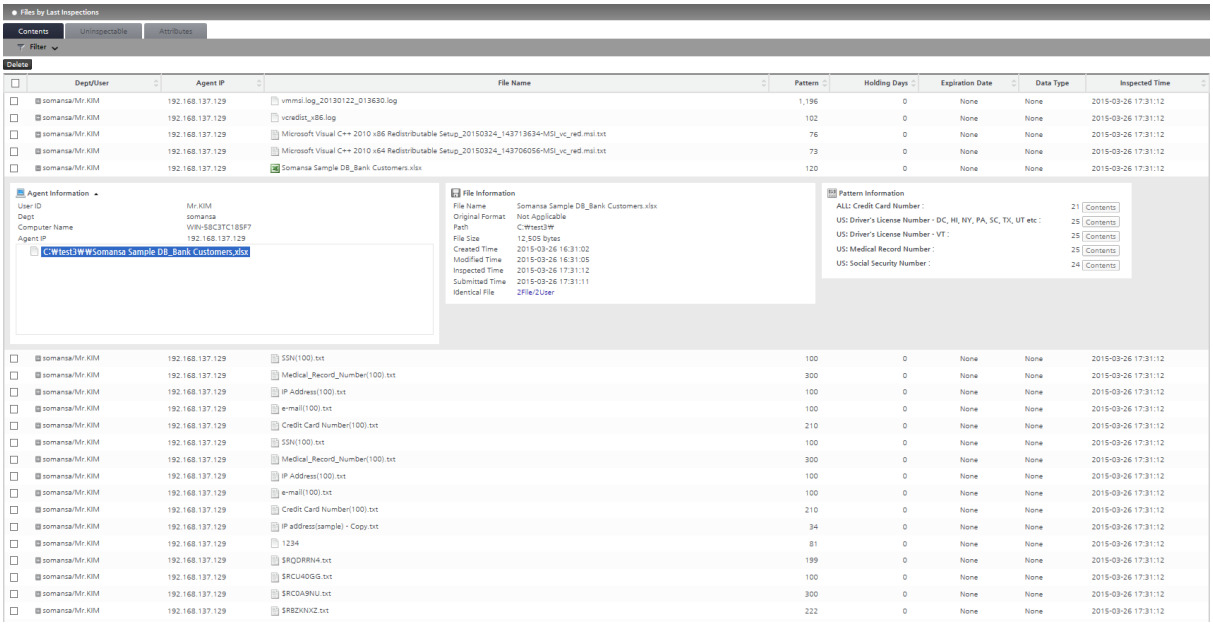
4.3 Incidents

4.3.1 Discover

4.3.1.1 PCs

- Files by Last Inspections

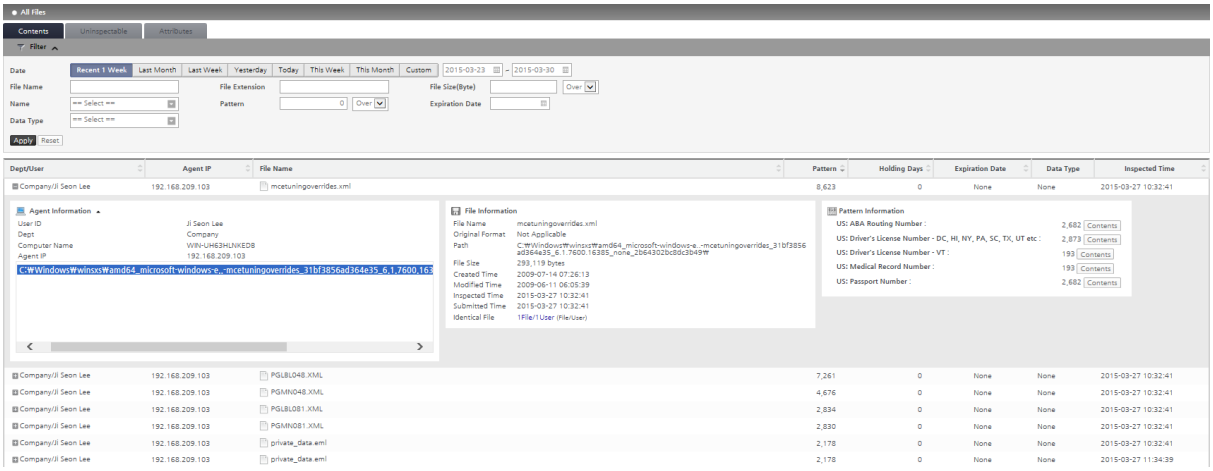
The data file details of departments and users that were most recently inspected can be viewed.



(FIGURE 4-24) DETECTED DATA RESULTS SCREEN

- All Files

The data file details of departments and users that were previously inspected can be viewed.



(FIGURE 4-25) FILE INSPECTION HISTORY SCREEN

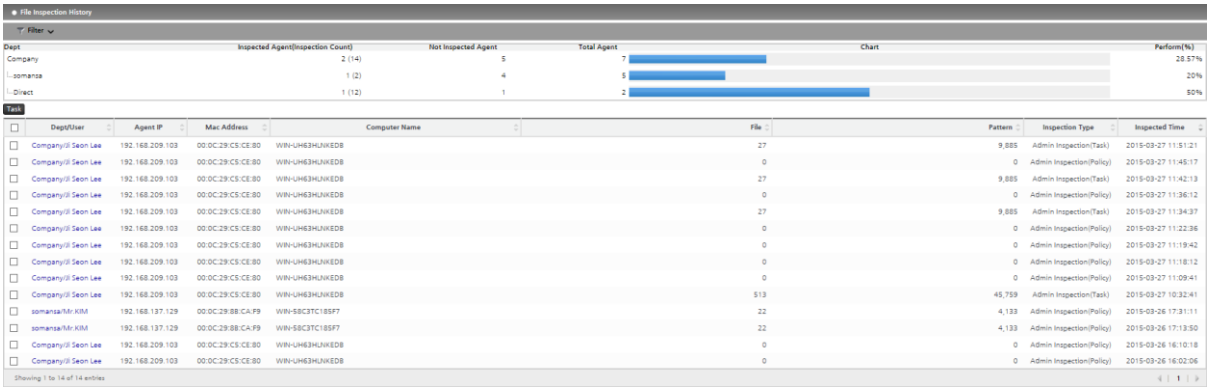
SOMANSA Copyright©2015 SOMANSA All rights reserved

[TABLE 4-3] ITEMS PROVIDED BY DISCOVER

Item	Description
Dept Name/ User Name	Set department and user name in the department
Agent IP	User IP
File Name	Detected file name
Number of Patterns	Numbers that include data patterns of the detected files
Retention Day	Number of days that a user retained the detected files
Expiration Date	Expiration date of the detected files
Information Type	Set information type of the detected files
Inspection Date	Date of the inspection

- File Inspection History

File inspection history and inspection (%) can be viewed. Use the View Results button on the right side to check the inspection results.



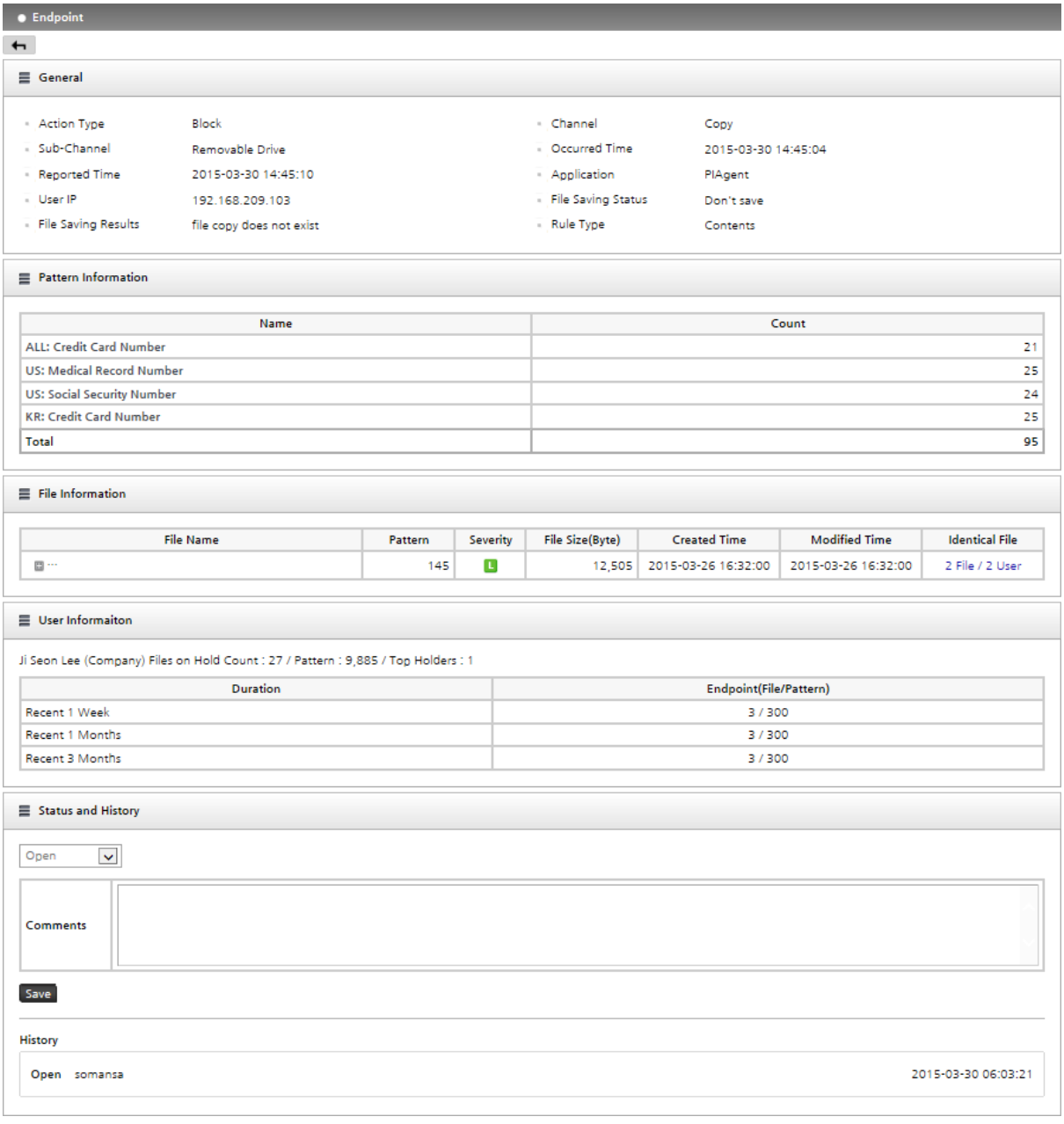
(FIGURE 4-26) FILE INSPECTION HISTORY SCREEN

4.3.2 Endpoint

Displays an exported or blocked file according to the channel and pattern conditions by a user or department. Through View Information, details of an exported file (Figure 4-28 above) can be viewed. By searching a similar file, files with the same confidential data based on a user can be viewed (Figure 4-28 below).

SOMANSA Copyright©2015 SOMANSA All rights reserved

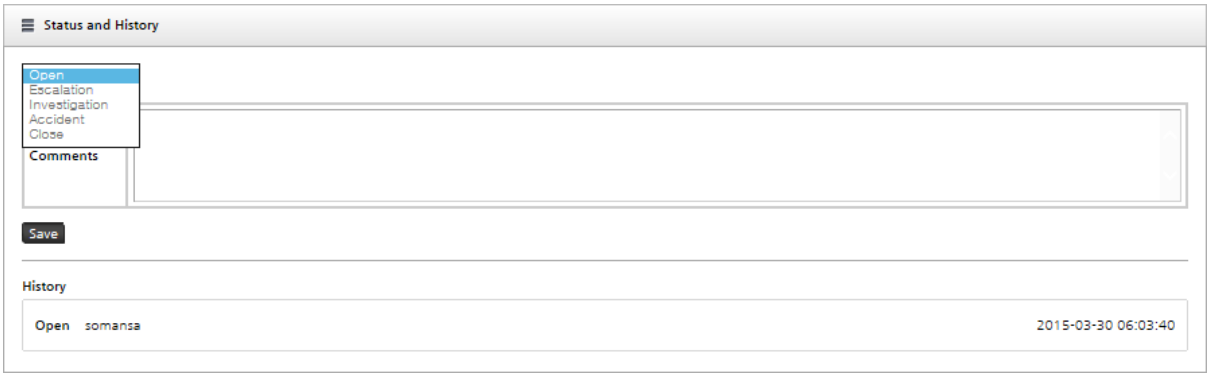
(FIGURE 4-27) ENDPOINT HISTORY SCREEN



(FIGURE 4-28) RESULTS OF THE EXPORTED FILE (ABOVE) AND DETAILS (BELOW)

SOMANSA Copyright©2015 SOMANSA All rights reserved

The admin can change the status of Endpoint Incidents and leave a comment to manage in the detail screen. Select Parent Report status to forward the details through email. (※ Audit Logs of the block before logging into the agent are stored in the PC. After logging into the agent, it will be uploaded to the Incidents Endpoint.)



(FIGURE 4-29) STATUS CHANGE AND HISTORY REPORT FOR EXPORT/BLOCK

[TABLE 4-4] ITEMS PROVIDED BY ENDPOINT

Item	Description
Dept Name/ User Name	Set department and user name in the department
Event Type	Whether the file is blocked/ allowed
Group	Policy group
Category	Activity category of the detected files
Contents	Audit history for the detailed actions
Number of Patterns	Numbers that include data patterns in the files
Status	Status of the detected file
Date	Date of the action

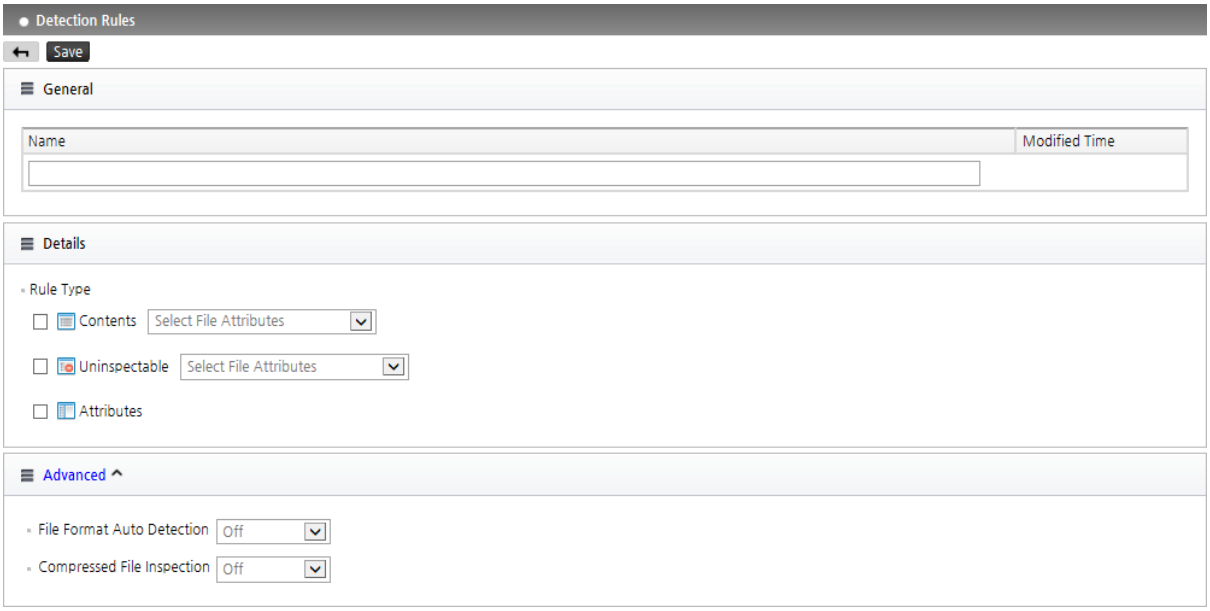
SOMANSA Copyright©2015 SOMANSA All rights reserved

4.4 Policy

Policy Management is categorized into Discover and Endpoint (Prevent). Discover manages the policy to inspect confidential data retained in the PC, and Endpoint manages the policy to control the flow of confidential data in the PC to external channels.

4.4.1 Detection Rules

Detection Rule for the Discover, Prevent+ Policy can be set. To create a Detection Rule, "File Attribute" Policy is required, and can be set based on Content, Uninspectable and Attribute. Attribute Policy can be viewed in the "Manage > Identifiers > File Attribute".



(FIGURE 4-30) DETECTION RULE SETTINGS SCREEN

☞ Policy Item Description

① Content: Detects based on the selected "File Attribute", Data Pattern and Number of Detection. During Inspection by Admin, the results are shown in "Contents".

② Uninspectable: "Unapproved Encryption File" can be selected. During Inspection by Admin, the results are shown in "Uninspectable" for an encrypted document or a compressed file.

SOMANSA Copyright©2015 SOMANSA All rights reserved

③ Attribute: Detects based on the selected Policy in "File Attribute", not the data inspection. During Inspection by Admin, the results are shown in "Attribute".

☞ Effective Input Field Range

[TABLE 4-5] EFFECTIVE INPUT FIELD RANGE FOR DETECTION RULES

Item	Effective Range	Character
Name	1~120	Numbers, uppercase/ lowercase letters, special characters

4.4.2 Discover

Discover provides a function to manage the policy to be used for inspecting confidential data retained in a PC.

4.4.2.1 PC

A policy that is used when inspecting confidential data retained in a user PC. Confidential Data Inspection Policy is categorized into a part to create a policy and a part to set a pattern. In the part to set a policy, a basic pattern and policy name can be set. In the part to set a pattern, a user-defined pattern other than the basic pattern can be added, or an expiration date of pattern can be added or modified. Click the policy on the list to see Policy Name/ Modified Time/ Number of Set Data Patterns at the bottom of the window. Please refer to [Table 4-6] for a description of each setting.

☞ Policy Item Description

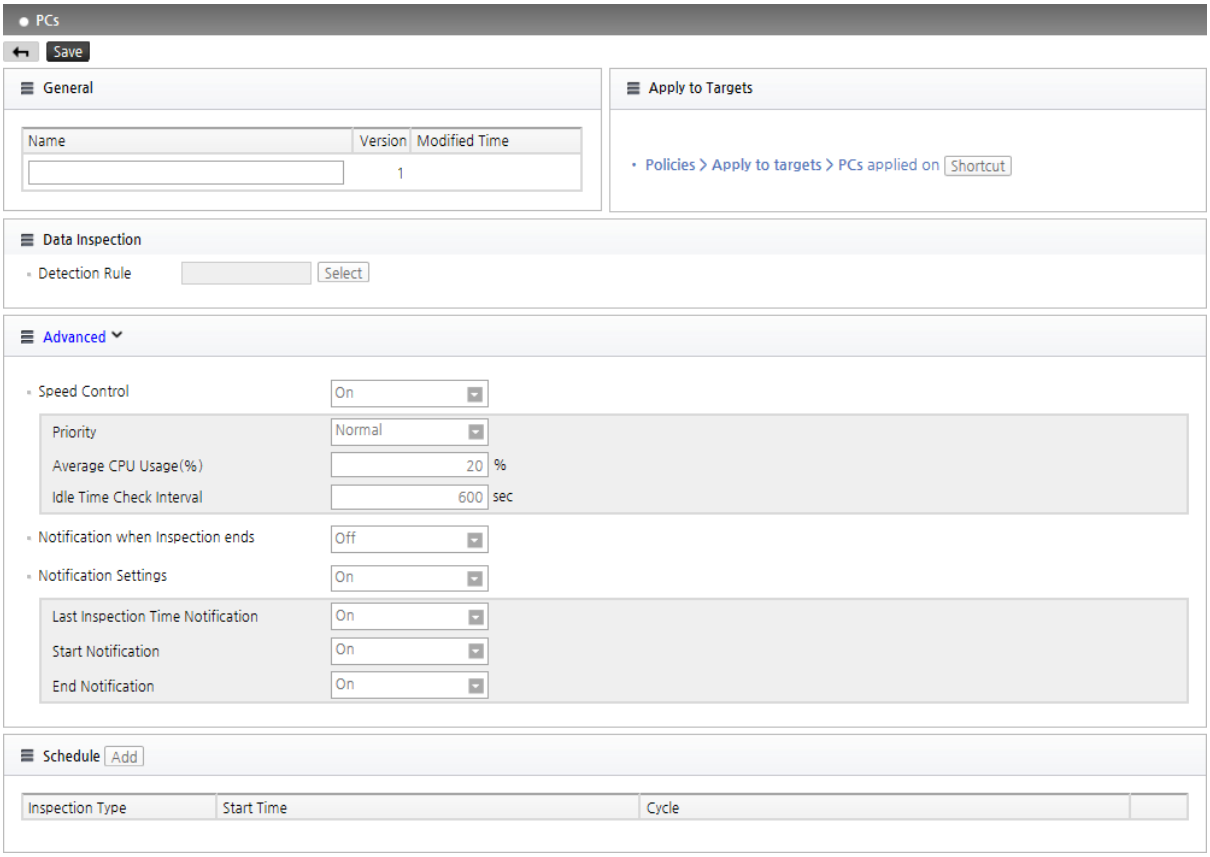
[TABLE 4-6] CONFIDENTIAL DATA INSPECTION OPTION SETTINGS

Category	Target	Description
Inspection Speed Settings	Inspection Speed Settings	Whether to set inspection speed or not
	Inspection Task Priority	High, Medium, Low
	Average CPU Allocation (%)	CPU resource settings when inspecting
	Idle Time Check Interval (seconds)	Uses maximum CPU if there is no mouse or keyboard input.

SOMANSA Copyright©2015 SOMANSA All rights reserved

Actions When Inspection is Complete	Popup Message	At the end of the inspection, the authorized person receives a popup message.
	Message Exposure Standard	Sets the number of detected patterns/ files with the popup message setting option.
Notification Settings	Automatic Notification for Last Inspection Time	Uses a notification message when terminating the final inspection of several Inspections by Admin.
	Notification for Starting Scheduled Task	Uses a notification message when starting a scheduled task.
	Notification for Terminating Scheduled Task	Uses a notification message when terminating a scheduled task
Schedule Settings	Inspection Type	Inspection target that performs file inspection.
	Start Date	Inspection start date
	Start Date and Time	Inspection start date and time
	Cycle	Inspection cycle can be run once, daily, weekly or monthly.

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 4-31) DISCOVER POLICY DETAILS SCREEN

☞ Item Description

① Detection Rule: Runs a data inspection, based on the registered policy in the "Detection Rules".

② Inspection Speed Control Function: A resource of the system can be specified for the process running inspection on an agent PC during Inspection by Admin. The setting for details is available when this function is set to use.

- Inspection Task Priority: Priority for the running process can be specified.
- Average CPU utilization allocated to inspection: CPU utilization of the running process can be set when running an inspection.
- Idle Time Check Interval: If an idle time set by a user PC has passed, the CPU utilization of the process becomes 100%. Inspection speed is improved through resources of the system that are not used during idle time.

SOMANSA Copyright©2015 SOMANSA All rights reserved

③ Popup Message When Terminating Inspection: A popup message can be provided to a user PC when Inspection by Admin is completed. The message is displayed according to a set pattern or number of files.

④ Notification Settings: Provides a notification window in the lower right corner when Inspection by Admin is completed. The settings for detailed items are available when this function is set to use.

- Notification for Last Inspection Date and Time: Displays the last inspection date.
- Notification for Starting Scheduled Task: Informs an agent PC that inspection has started when a scheduled task starts.
- Notification for Terminating Scheduled Task: Informs an agent PC that inspection was terminated when a scheduled task terminates.

☞ Effective Input Field Range

[TABLE 4-7] EFFECTIVE INPUT FIELD RANGE FOR POLICY PC

Item	Effective Range	Character	Failure Message
Name	1~120	Numbers, uppercase/ lowercase letters, special characters	Enter policy name.
Average CPU Utilization Allocated to Inspection	0~100	Numbers	Only numbers between 10 and 100 can be entered.
Idle Time Check Interval	0~999	Numbers	A number less than 1 cannot be entered.

4.4.3 Endpoint

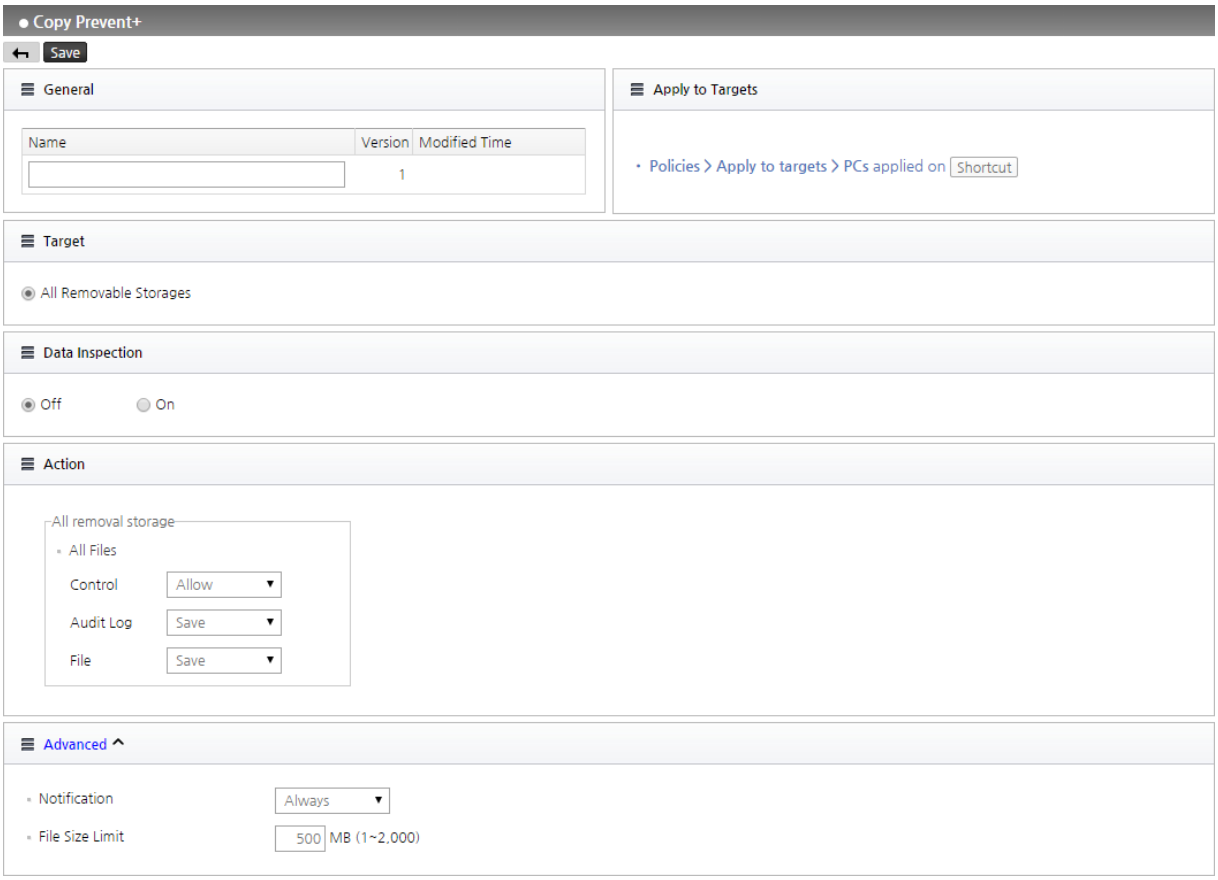
In the Endpoint, a policy can be defined for controlling channels that can communicate externally, such as removable storage devices, communication media, printers, application programs, networks, etc. A policy that logs or blocks when a user transfers a confidential file

SOMANSA Copyright©2015 SOMANSA All rights reserved

externally can be specified. A leak of important company information can be prevented in advance.

4.4.3.1 Copy Prevent+

A policy can be set for removable storage devices including USB drives. The other data leakage control policies below are configured with the same process. Since a wide range of USBs are used in a company, it is often difficult to manually apply and allow or block policy for available USB drive restriction.



(FIGURE 4-32) COPY PREVENT POLICY DETAILS SCREEN

☞ Policy Item Description

① Target: 'All Removable Storage Devices' can be selected, and the policy for the all removable storage device is registered.

② Data Inspection: 'Off' or 'On' can be selected. When 'On' is selected, the policy

SOMANSA Copyright©2015 SOMANSA All rights reserved

registered in "Detection Rules" can be selected, and the policy is set according to the specified rule.

③ Action: 'All Removable Storage Devices' can be set to allow/block. In addition, 'Save/ Do Not Save' can be set for a copied file when allowed.

④ Notification Message: 'No Notification', 'Always Notify', and 'Notify When Blocked' can be selected. Notification on Privacy-i Agent will be shown when it's set.

⑤ Copy Size Limit: Only a copy of the set value can be saved when saving a copy.

☞ Effective Input Field Range

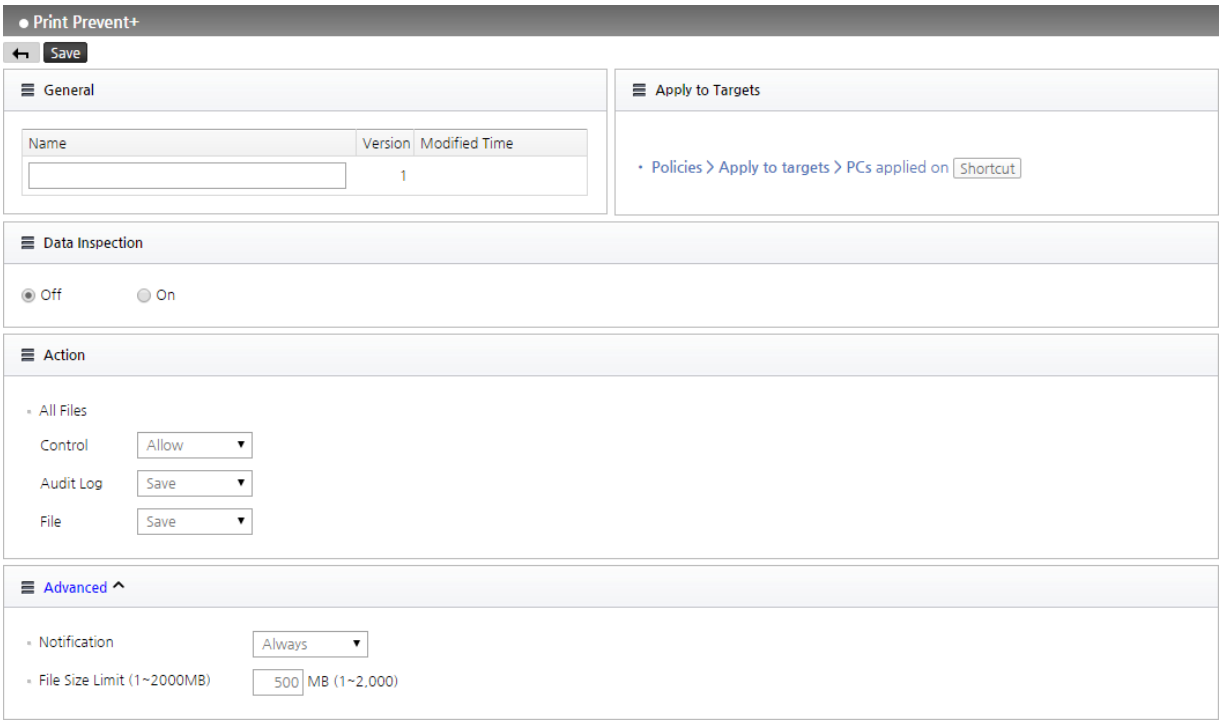
[TABLE 4-8] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING REMOVABLE STORAGE DEVICES

Item	Effective Range	Character	Failure Message
Name	1~120	Numbers, uppercase/ lowercase letters, special characters	Enter a policy name.
Copy Size Limit	1~2000	Numbers	Only values between 1MByte to 2000Mbytes can be entered for the copied file size.

SOMANSA Copyright©2015 SOMANSA All rights reserved

4.4.3.2 Print Prevent+

Sets a policy for printing documents. Other data leakage control policies below are configured with the same process.



(FIGURE 4-33) PRINT PREVENT DETAILS SCREEN

☞ Policy Item Description

① Data Inspection: 'Off' or 'On' can be selected. When 'On' is selected, the policy registered in "Detection Rules" can be selected, and the policy is set by the specified rule.

② Action: All files that are printed can be set to allow/ block. In addition, 'Save/ Do Not Save' can be set for a copied file when allowed.

③ Notification Message: 'No Notification', 'Always Notify', and 'Notify When Blocked' can be selected. Notification will be shown on Privacy-i Agent when it is set.

④ Copy Size Limit: Only a copy of a set value can be saved when saving a copy.

SOMANSA Copyright©2015 SOMANSA All rights reserved

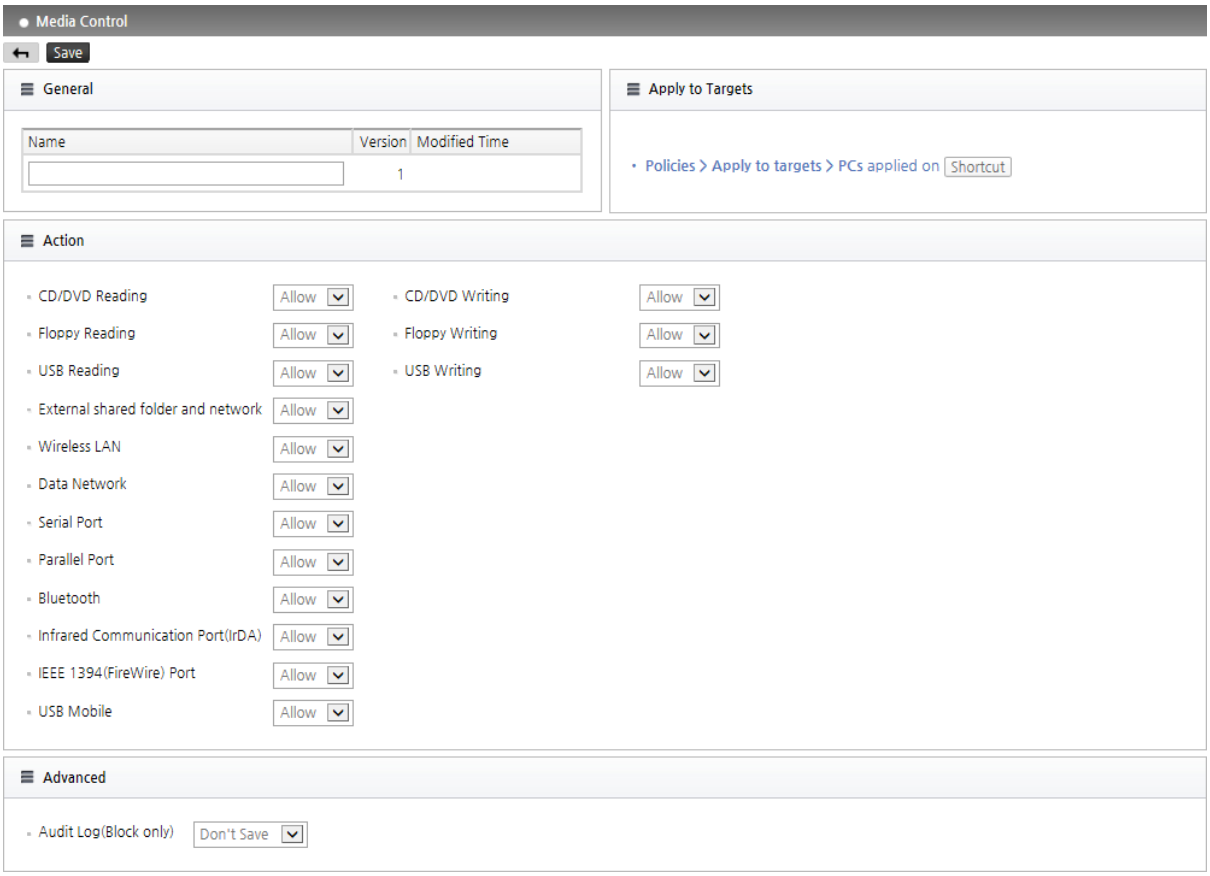
☞ Effective Input Field Range

[TABLE 4-9] EFFECTIVE INPUT FIELD RANGE FOR PRINT PREVENT

Item	Effective Range	Character	Failure Message
Name	1~120	Numbers, uppercase/ lowercase letters, special characters	Enter a policy name.
Copy Size Limit	1~2000	Numbers	Only values between 1MByte to 2000MBytes can be entered for the copied file size.

4.4.3.3 Media Control

Privacy-i provides a Control function to allow or block data from moving to external channels, such as CD/DVDs and floppy disk reading/writing, external shared folder and network drive connections, wireless LAN, data networks (tethering, Wibro), serial/parallel ports, Bluetooth, infrared communication (IrDA), IEEE 1394 (Firewire), USB removable devices (USB Mobile), etc.



(FIGURE 4-34) MEDIA CONTROL DETAILS SCREEN

SOMANSA Copyright©2015 SOMANSA All rights reserved

☞ Policy Item Description

① Control Settings: CDs/DVDs, floppy disks and USBs can be divided into reading and writing, and set to be allowed/ blocked. Reading other specified media is blocked/ allowed.

☞ Effective Input Field Range

[TABLE 4-10] EFFECTIVE INPUT FIELD RANGE FOR MEDIA

Item	Effective Range	Character	Failure Message
Name	1~120	Numbers, uppercase/ lowercase letters, special characters	Enter a policy name.

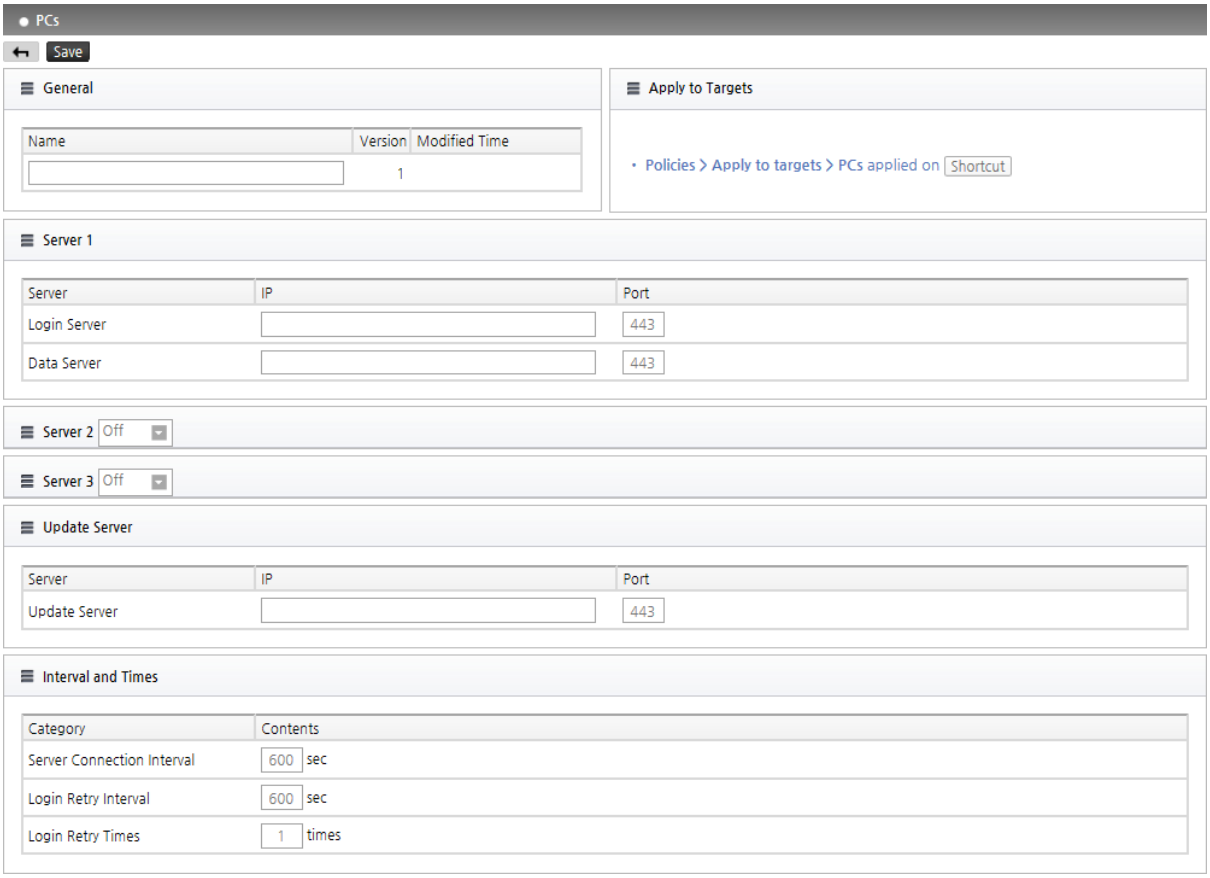
4.4.3.4 Policy Application Time

A function to set a time frame to apply online or offline policies

4.4.4 Connections

Configures connection settings for the server where an agent can connect.

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 4-35) PC CONNECTION SETTINGS SCREEN

☞ Policy Item Description

① Connection Server 1: Configures connection server for Privacy-i Agent.

- Connection Server 2 (3): Can be set the same way as Connection Server 1 when selected to use. This setting item is required for Dual or Triple Redundancy Settings.

② Server Connection Interval: Sets an interval time to connect to the server.

③ Login Retry Interval: Sets a re-login time if there is no response from a PC with Privacy-i Agent installed.

④ Login Retry Attempts: Sets number of login retries when account fails.

☞ Effective Input Field Range

SOMANSA Copyright©2015 SOMANSA All rights reserved

[TABLE 4-11] EFFECTIVE INPUT FIELD RANGE FOR CONNECTIONS

Item	Effective Range	Character	Failure Message
Name	1~120	Numbers, uppercase/ lowercase letters, special characters	Enter a setting name.
IP	15	Numbers, special characters (.) (However, 0.0.0.0 and 255.255.255.255 cannot be entered.)	Incorrect IP was inserted on Connection Server 1. Try again after checking.
Server Connection Interval	1~99999	Numbers	Spaces cannot be entered.
Login Retry Interval	1~99999	Numbers	Spaces cannot be entered.
Login Retry Times	1~99999	Numbers	Spaces cannot be entered.

4.4.5 Apply to Targets

4.4.5.1 PCs

Discover, Prevent+ and Connections Policies are applied to a department and user.

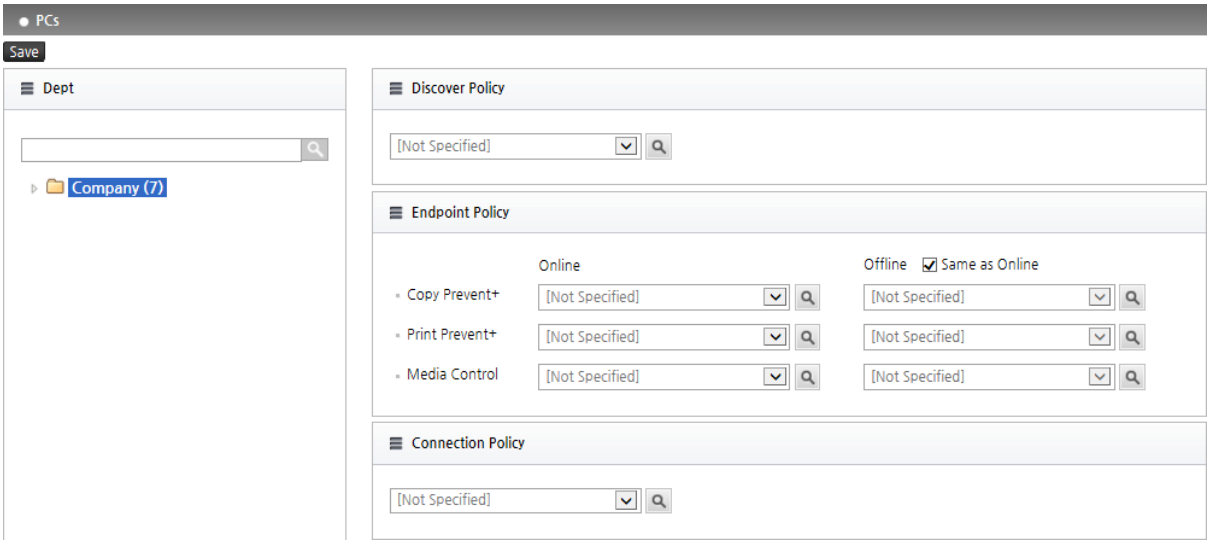
* If it is a default policy, all items in [Table 4-12] will be blocked.

Notice

✓ If Copy Prevent+ Policy and Media Control Policy are set at the same time, Copy Prevent+ Policy takes precedence.

✓

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 4-36) POLICY APPLICATION SETTINGS SCREEN

☞ Effective Input Field Range

[TABLE 4-12] EFFECTIVE INPUT FIELD RANGE FOR APPLY TO TARGETS

Item	Effective Range	Character	Failure Message
Find	1~100	Numbers, uppercase/ lowercase letters, special characters	-

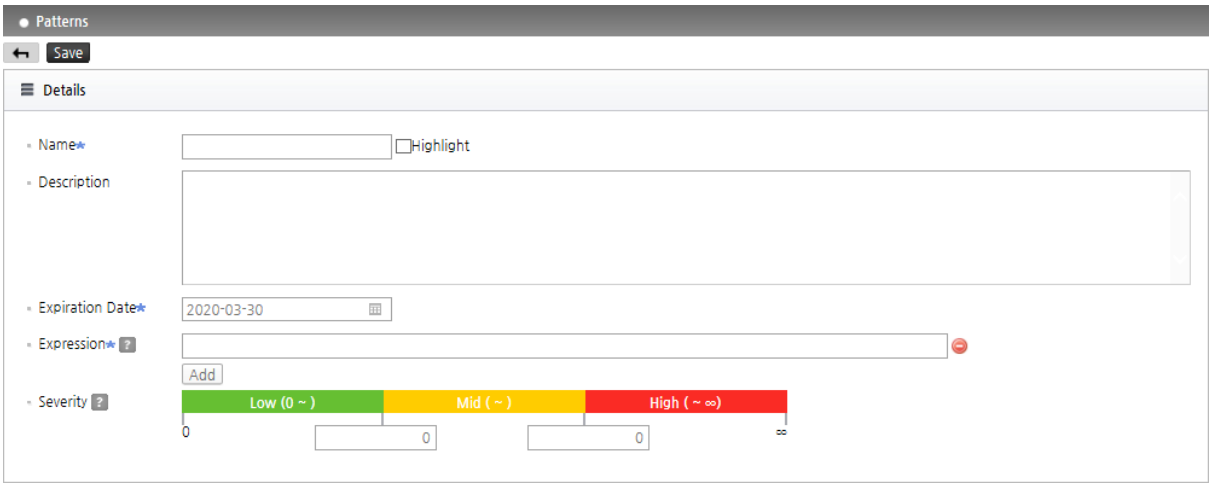
SOMANSA Copyright©2015 SOMANSA All rights reserved

4.5 Manage

4.5.1 Identifiers

4.5.1.1 Pattern

In Pattern, basic patterns of confidential data provided by SOMANSA can be viewed. Provided patterns include social security number, driver's license number, credit card number, health insurance card number, passport number, account number, cell phone number, phone number, IP address, and E-mail address, and more. When detecting a specific phrase or pattern, a user-defined pattern can be generated. Basic patterns cannot be deleted, and expressions cannot be modified or deleted. Pattern is used when creating Inspection Policy in Policy Management and Discover.



(FIGURE 4-37) PATTERN DETAILS SCREEN

☞ Policy Item Description

① Expiration Date: Sets an expiration date for the currently registered pattern.

② Expression: Sets a pattern to detect through a general keyword or regular expression.

③ Severity: Sets a severity when detecting a pattern.

SOMANSA Copyright©2015 SOMANSA All rights reserved

☞ Effective Input Field Range

[TABLE 4-13] EFFECTIVE INPUT FIELD RANGE FOR PATTERN

Item	Effective Range	Character	Failure Message
Name	3~225	Numbers, uppercase/ lowercase letters, special characters	A pattern name should have at least 3 characters.
Description	1~225	Numbers, uppercase/ lowercase letters, special characters	-
Expression	1~200	Numbers, uppercase/ lowercase letters, special characters	A blank value cannot be registered in the expression.
Severity	0~999,999,999	Numbers	0 cannot be entered in Severity Settings.

4.5.1.2 File Format

Manages a format to use in file attributes

* However, unsupported formats cannot be detected, and logs cannot be stored.

[TABLE 4-14] DEFAULT INSPECTION FORMAT FILE

Order	File Type	Category	Format Name	Extension
1	Text	Basic Format	Copy of Printed Document	pvi
2			Microsoft Hypertext Archive	mht
3			Hypertext Markup Language	html;htm
4			Extensible Markup Language	xml
5			Rich Text Format	rtf
6			Comma-Separated Values	csv
7			Plain Text Format	txt
8	Word processor	Basic Format	iWork Pages	pages
9			Corel WordPerfect	wpd;wp;wp4;wp5;wp6;wp7
10			OpenOffice Writer	odt;sxw
11			Hancom HWP	hwp
12			HandiSoft Arirang	hwd

SOMANSA Copyright©2015 SOMANSA All rights reserved

13			Microsoft Word	doc;docx
14	Spreadsheet	Basic Format	iWork Numbers	numbers
15			OpenOffice Calc	ods;sxc
16			Microsoft Excel	xls;xlsx;xlsm
17	Presentation	Basic Format	Hancom Office Hanshow	show
18			iWork Keynote	key
19			OpenOffice Impression	odp;sxi
20			Microsoft PowerPoint	ppt;pptx;pps
21	E-mail	Basic Format	Microsoft Outlook Express	eml;mht
22			Microsoft Outlook	msg;oft
23	Database	Basic Format	Microsoft Access	mdb;accdb
24	Others	Basic Format	XML Paper Specification	xps
25			Microsoft Compiled HTML	chm
26			Adobe Portable Document Format	pdf

☞ Policy Item Description

① File Type: Specified file types can be selected. Desired file types can be entered when directly selecting Add.

② File Extension: Desired file extensions can be entered when detecting a file. The extensions provided by default are listed in [Table 4-14].

☞ Effective Input Field Range

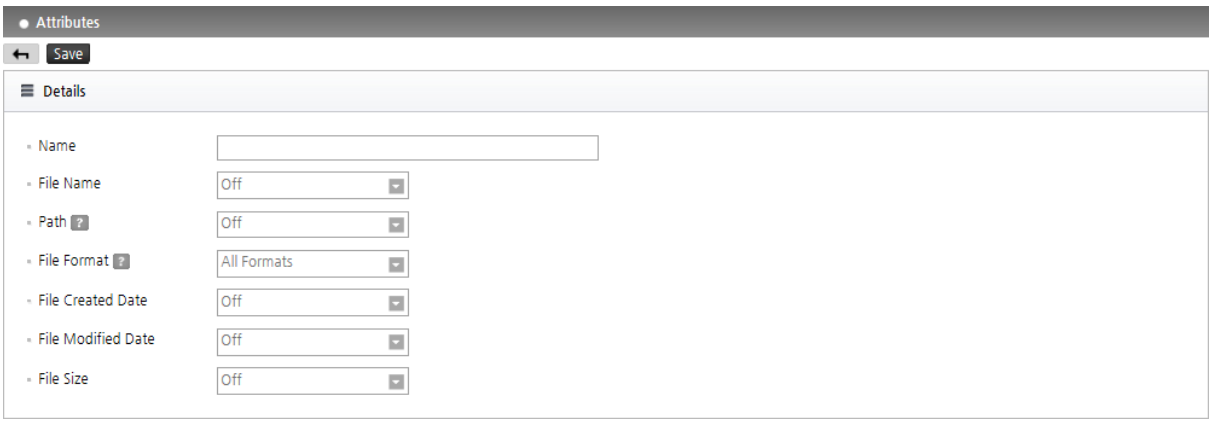
[TABLE 4-15] EFFECTIVE INPUT FIELD RANGE FOR FILE FORMAT

Item	Effective Range	Character	Failure Message
Name	1~225	Numbers, uppercase/ lowercase letters, special characters	Enter a format name.
File Extension	1~20	Letters	An empty value cannot be registered for file type.

SOMANSA Copyright©2015 SOMANSA All rights reserved

4.5.1.3 Attributes

In Attributes, a condition value of a file attribute to be inspected can be specified. Inspection can be carried out according to file name, path, type, date created and size. To create a policy, one or more conditions must be selected. Each setting satisfies the AND condition, and a file is detected according to the settings for each item. A generated file attribute is used when creating a policy in Policy Management and Discover.



(FIGURE 4-38) FILE ATTRIBUTE DETAILS

☞ Policy Item Description

① File Name: When selected, the file name field is activated, and Included Target and Excluded Target can be selected. A file name to detect (exclude) can be entered. A file name must be entered with its extension.

② Path: When selected, the path name field is activated, and Included Target and Excluded Target can be selected. A path to detect (exclude) can be entered.

③ File Format: All Formats or Specify Directly can be selected. When Specify Directly is selected, the desired format among formats described in [Table 4-21] can be selected.

④ File Created Date: When selected, the date field is activated, and date created to detect can be selected.

⑤ File Modified Date: When selected, the date field is activated, and date modified to detect can be selected.

⑥ File Size: When selected, the field size is activated, and file size to detect can be

SOMANSA Copyright©2015 SOMANSA All rights reserved

entered. Size is divided into a range and minimum for selection.

☞ Effective Input Field Range

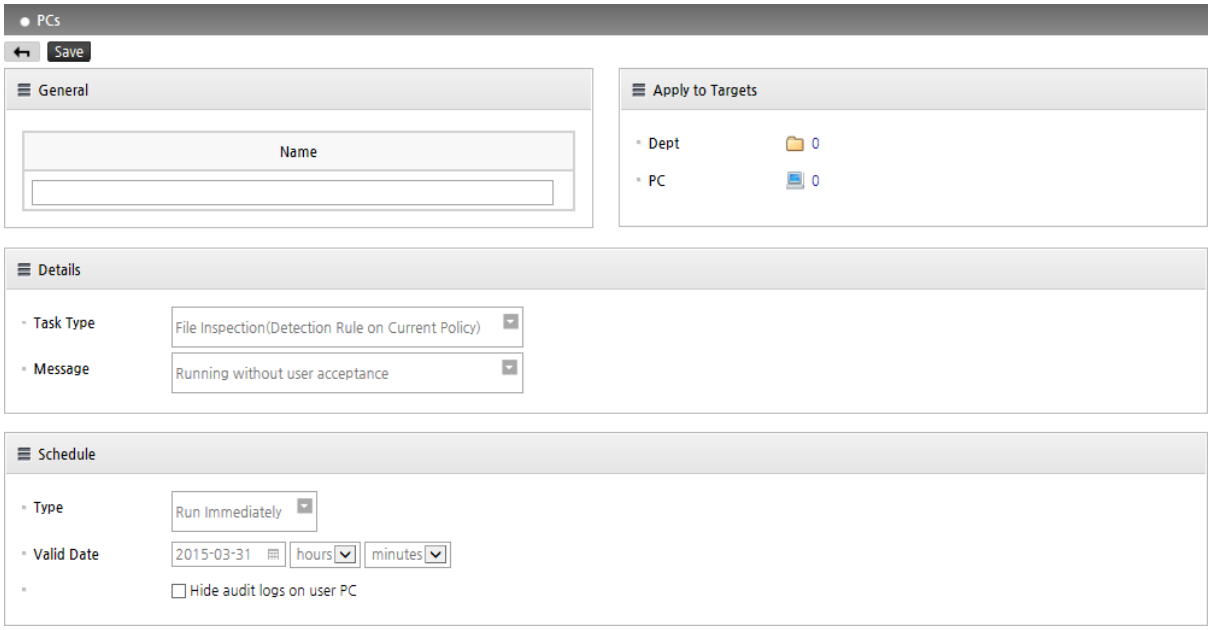
[TABLE 4-16] EFFECTIVE INPUT FIELD RANGE FOR FILE ATTRIBUTES

Item	Effective Range	Character	Failure Message
Name	3~225	Numbers, uppercase/ lowercase letters, special characters	Name should have at least 3 characters.

4.5.2 Admin Action

4.5.2.1 PC

Manages confidential data on a user PC and agent environment for a user or department. Types provided with a remote command include Inspection by Admin, Delete File, Server Connection Policy Update and Agent Update. Schedule settings are available to run a task temporarily or repeatedly. Forced execution without user consent or executing a task with user consent can be set.



(FIGURE 4-39) TASK SETTINGS SCREEN

SOMANSA Copyright©2015 SOMANSA All rights reserved

[Table 4-17] below contains detailed information about remote command types.

Remote Command Types	Description
File Inspection (Detection Rule on Current Policy)	Runs confidential data inspection with the Inspection Policy assigned to a department or user
File Inspection (Temporary Detection Rule)	Runs confidential data inspection with another policy, not the Inspection Policy assigned to a department or user.
File Delete	Deletes files from the latest inspection results.
Update Connection Policy	A task that is run on an agent when Server Connection Policy is modified.
Agent Update	Transfers an update command to a user when the agent update module is configured on the server.
Cancel for Inspection in progress	Cancels an inspection that is currently running on an agent.

[TABLE 4-17] TASK TYPES AND FUNCTIONS

☞ Policy Item Description

① Task Type: Specified in Remote Command Types and Functions in [Table 4-37], and runs a selected task.

- File Inspection (Detection Rule on Current Policy): Sets a task with a policy specified for a user in POLICIES > Apply to Targets.
- File Inspection (Temporary Detection Rule): Sets a task with a rule specified in "Detection Rules" item, which appears when selecting.
- File Delete: Sets a task that selects the detected file of a user (department) chosen in "Target" and deletes the file through the "Add File" button, which appears when selecting.
- Update Connection Policy: Server Policy can be updated by selecting the

SOMANSA Copyright©2015 SOMANSA All rights reserved

desired settings in "Update Target", which appears when selecting.

- Cancel for Inspection in progress: A policy to cancel an Inspection by Admin that is currently running can be registered.

② Details: A task for a user or department can be specified. Execution without user consent or a user consent request can be selected. When selecting a user consent request, a message for a consent request can be entered.

③ Schedule: Running methods include an immediate execution or scheduled execution. A scheduled execution runs a task on a scheduled date and time. When selecting audit logs to be hidden in a user PC, the audit logs do not remain in the agent.

☞ Effective Input Field Range

[TABLE 4-18] EFFECTIVE INPUT FIELD RANGE FOR CONTROL BY ADMIN

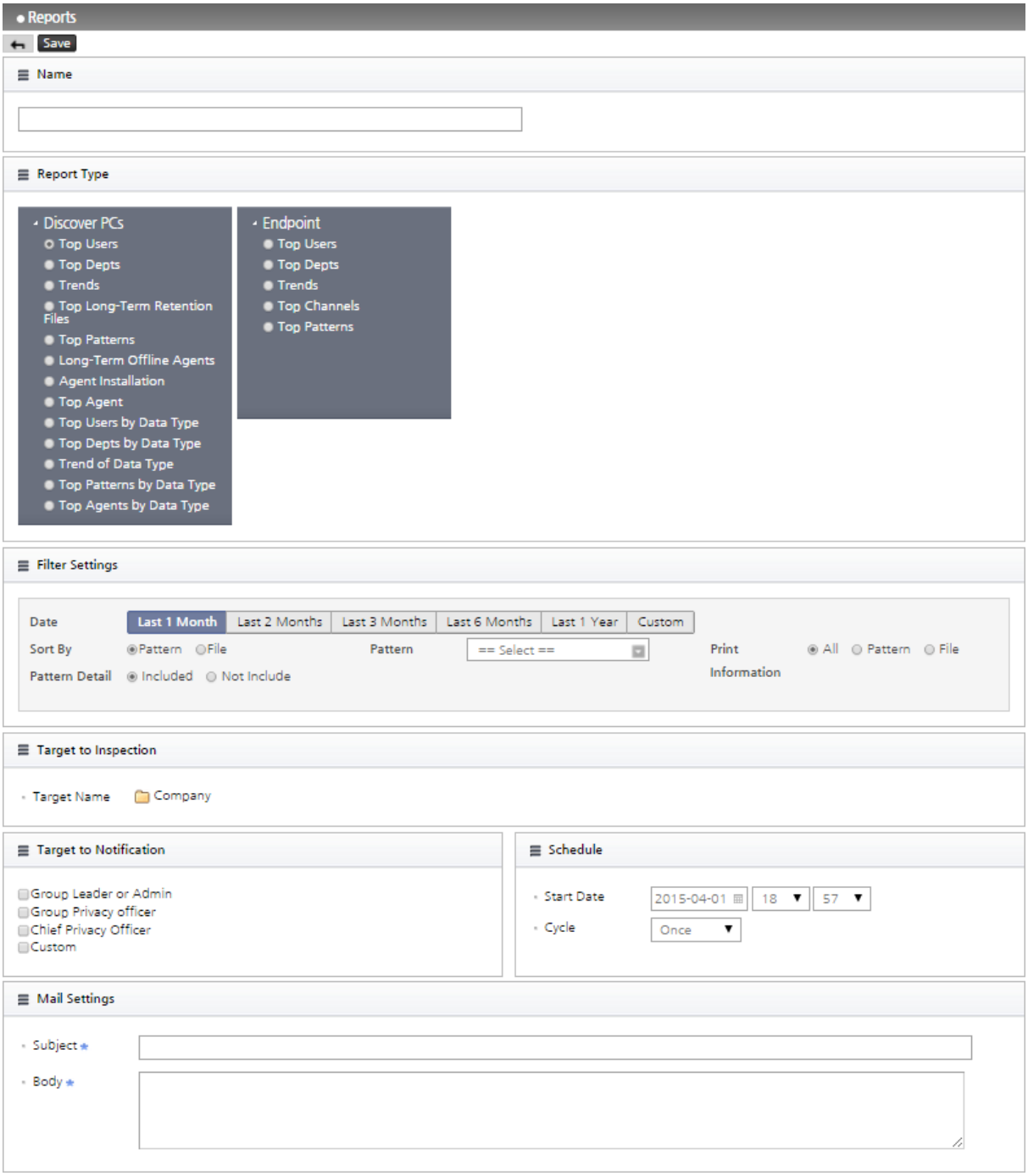
Item	Effective Range	Character	Failure Message
Name	1~120	Numbers, uppercase/ lowercase letters, special characters	Enter a task name.
Message	1~4000	Numbers, uppercase/ lowercase letters, special characters	-

4.5.3 Alerts/Notification

4.5.3.1 Reports

Statistics of Discover and Endpoint can be sent to the E-mail registered in user information.

SOMANSA Copyright©2015 SOMANSA All rights reserved

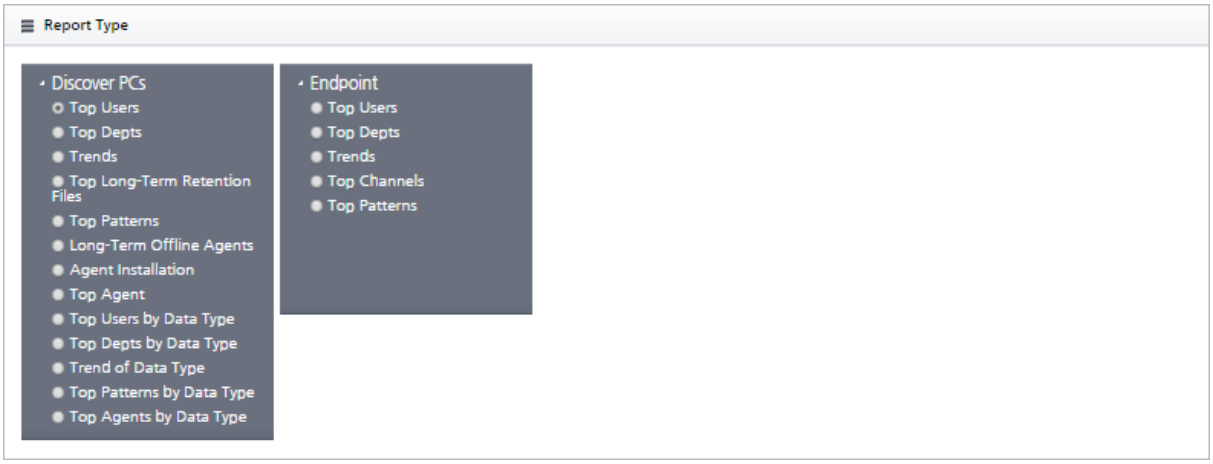


(FIGURE 4-40) REPORT NOTIFICATION DETAILS SCREEN

☞ Report Notification Details

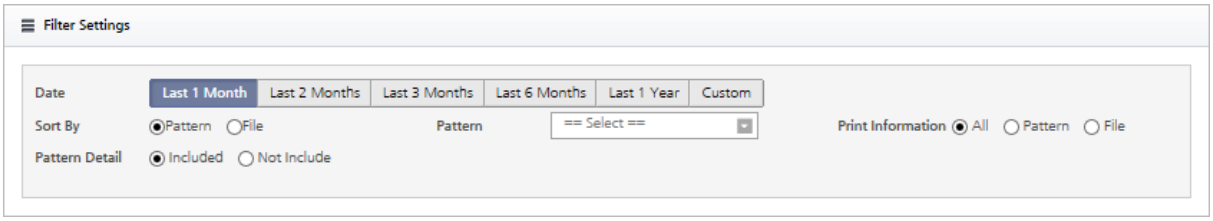
- Report Type: One of the report details of Discover PCs, Discover Servers and Endpoint DLP can be selected.

SOMANSA Copyright©2015 SOMANSA All rights reserved



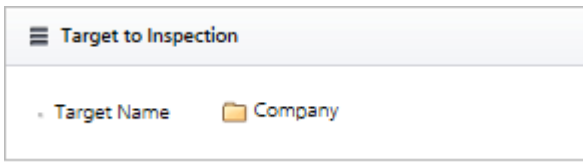
(Figure 4-41) Report Type Screen

- Filter Settings: Recent Inspection Date, Ranking Criteria and Pattern can be selected and a filter can be applied.



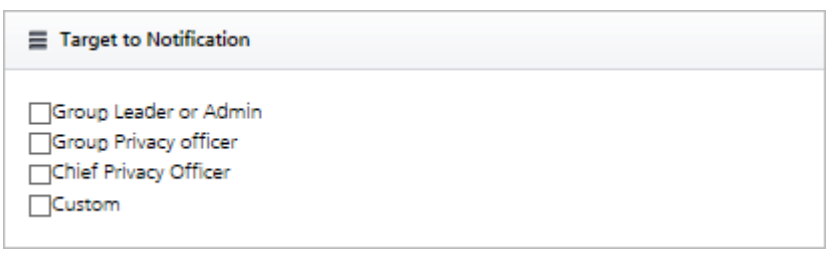
(Figure 4-42) Filter Settings Screen

- Target to Inspection: A department or a user can be selected for Inspection Summary Target.



(Figure 4-43) Target to Inspection Screen

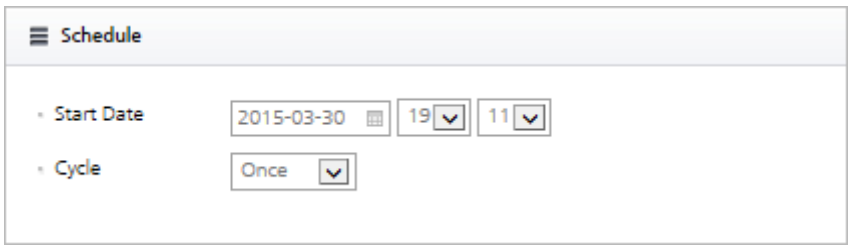
- Target to Notification: Notification target can be selected.



(Figure 4-44) Target to Notification Screen

SOMANSA Copyright©2015 SOMANSA All rights reserved

- Schedule: Notification cycle can be set once, daily, weekly or monthly.



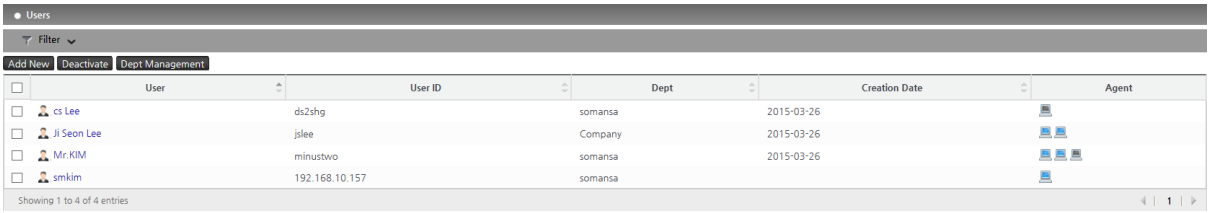
(FIGURE 4-45) NOTIFICATION CYCLE SETTINGS SCREEN

- Mail Settings: Mail subject and body can be entered.

(Figure 4-46) Mail Settings Screen

4.5.4 Users

A user can be added, modified and deleted. Number of agents retained and connection status can be viewed through the agent column on the list.

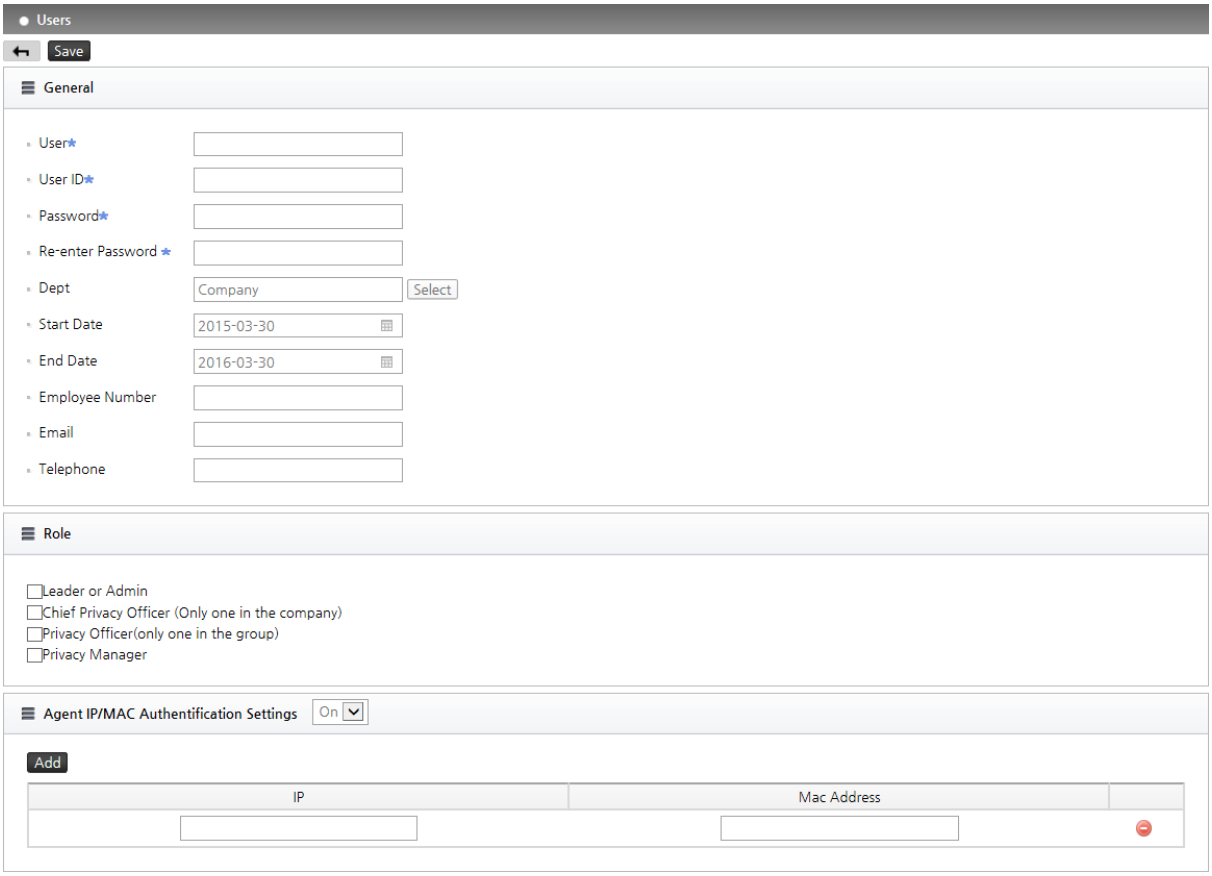


(Figure 4-47) User Account Management Screen

- User Management

User Management shows the agent information on a user PC that is registered to User Information. For user information, functions including adding, deleting a user, and changing a password are provided.

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 4-48) USER MANAGEMENT DETAILS

☞ Policy Item Description

① Dept: Department registered in "MANAGER > Users > Dept Management" can be selected, and a user is registered to the selected department.

② Start Date: An available start date of the account to register can be entered.

③ End Date: An available end date of the account to register can be entered.

④ Employee Number: Employee number of the account user to register can be entered.

⑤ Email: Email of the account user to register can be entered.

⑥ Telephone: Phone number of the account user to register can be entered.

☞ Effective Input Field Range

SOMANSA Copyright©2015 SOMANSA All rights reserved

[TABLE 4-19] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING USERS

Item	Effective Range	Character	Failure Message
User	1~225	Numbers, uppercase/ lowercase letters, special characters	Enter user name.
User ID	4~20	Numbers, uppercase/ lowercase letters, special characters	Enter user ID.
Password	9~35	Numbers, uppercase/ lowercase letters, special characters	Enter password.
Re-enter Password	9~35	Numbers, uppercase/ lowercase letters, special characters	There is no password confirmation value.
Employee Number	1~20	Numbers, uppercase/ lowercase letters, special characters	-
Email	1~50	Numbers, uppercase/ lowercase letters, special characters	-
Telephone	1~15	Numbers	-

Recommendations

✓ Password should have at least 9 characters and include English letters, numbers and special characters.

- Policy Management

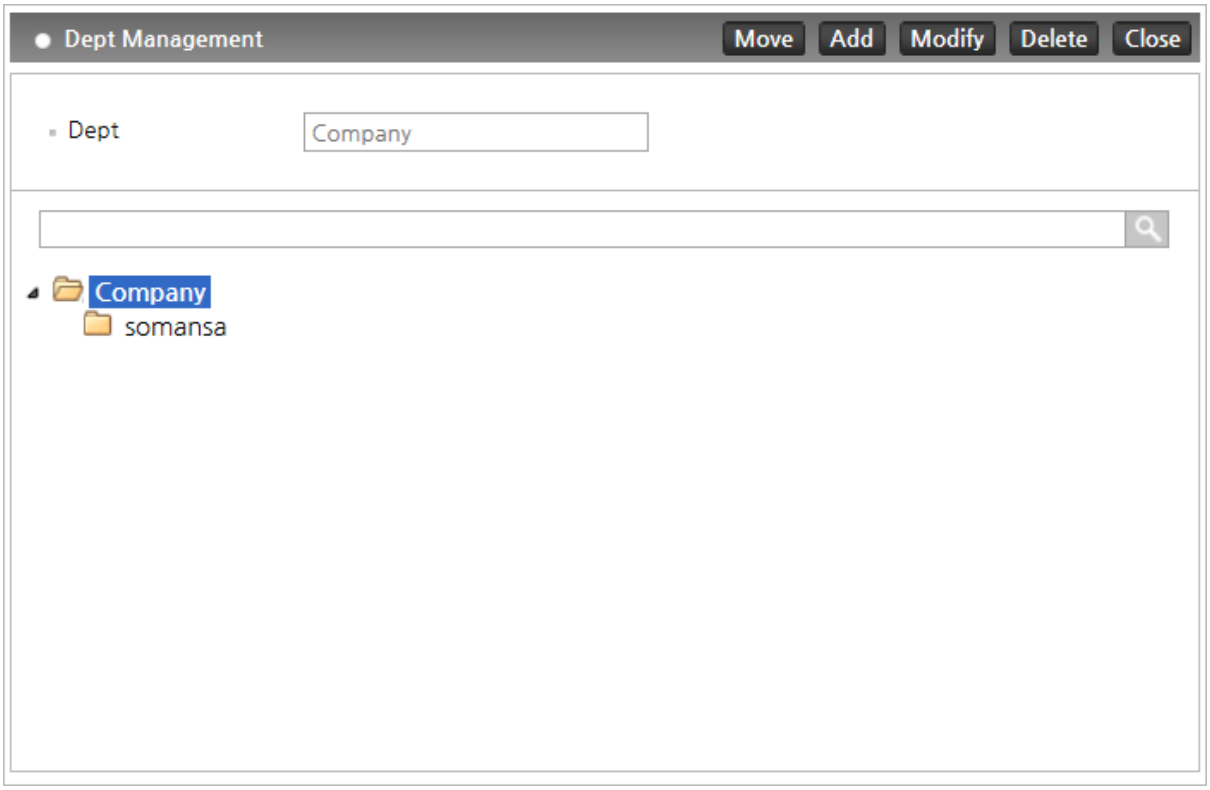
Discover Inspection Policy and Endpoint DLP Policy generated in policy can be specified by department or user.

- Dept Management

Dept Management shows departments registered in User Information. For user information,

SOMANSA Copyright©2015 SOMANSA All rights reserved

functions to add, delete and move department are provided.



(FIGURE 4-49) DEPT MANAGEMENT

☞ Effective Input Field Range

[TABLE 4-20] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING USERS DEPT

Item	Effective Range	Character	Failure Message
Dept	1~100	Numbers, uppercase/ lowercase letters, special characters	Enter a department name.
Find	1~100	Numbers, uppercase/ lowercase letters, special characters	-

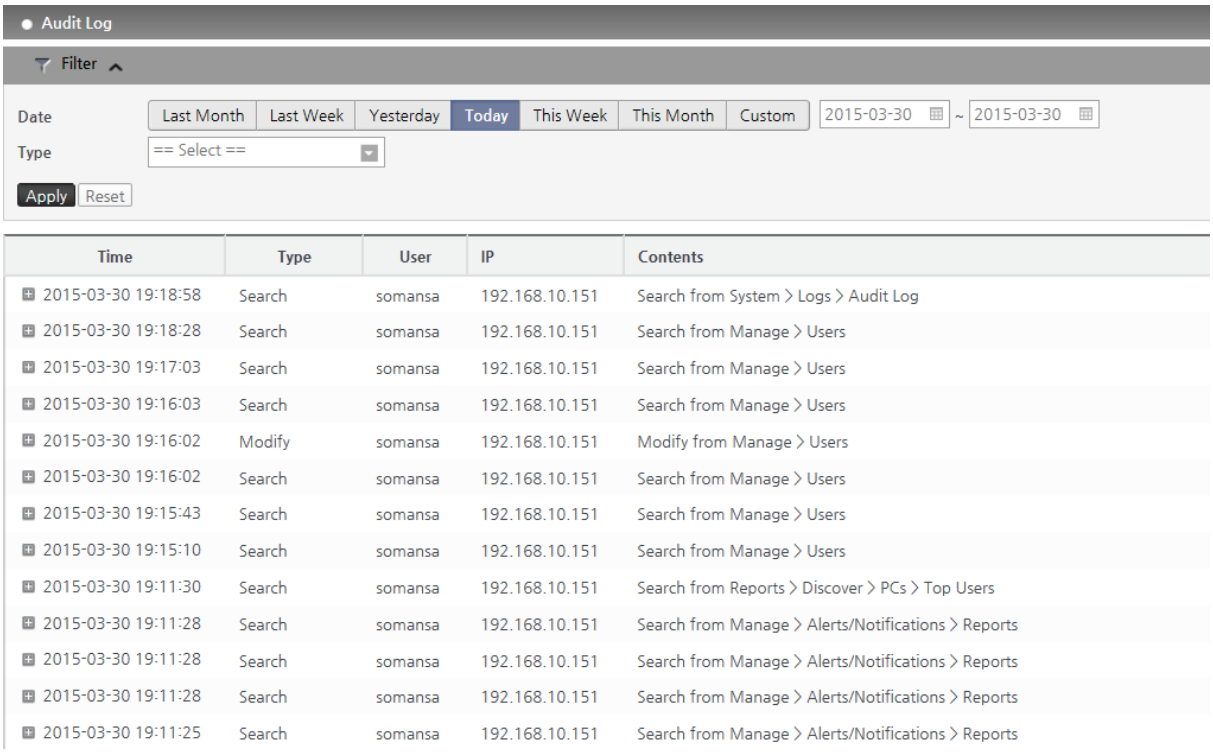
SOMANSA Copyright©2015 SOMANSA All rights reserved

4.6 System

4.6.1 Logs

- Audit Logs

For all activities of the admin, Information Management Logs, Information Trace Logs, Policy Management Logs and Account Management Logs can be viewed. An Audit Trail is provided through the log.


Audit Log
Filter
Date
Last Month
Last Week
Yesterday
Today
This Week
This Month
Custom
2015-03-30 ~ 2015-03-30
Type
== Select ==
Apply
Reset
Time
Type
User
IP
Contents
2015-03-30 19:18:58 Search somansa 192.168.10.151 Search from System > Logs > Audit Log
2015-03-30 19:18:28 Search somansa 192.168.10.151 Search from Manage > Users
2015-03-30 19:17:03 Search somansa 192.168.10.151 Search from Manage > Users
2015-03-30 19:16:03 Search somansa 192.168.10.151 Search from Manage > Users
2015-03-30 19:16:02 Modify somansa 192.168.10.151 Modify from Manage > Users
2015-03-30 19:16:02 Search somansa 192.168.10.151 Search from Manage > Users
2015-03-30 19:15:43 Search somansa 192.168.10.151 Search from Manage > Users
2015-03-30 19:15:10 Search somansa 192.168.10.151 Search from Manage > Users
2015-03-30 19:11:30 Search somansa 192.168.10.151 Search from Reports > Discover > PCs > Top Users
2015-03-30 19:11:28 Search somansa 192.168.10.151 Search from Manage > Alerts/Notifications > Reports
2015-03-30 19:11:28 Search somansa 192.168.10.151 Search from Manage > Alerts/Notifications > Reports
2015-03-30 19:11:28 Search somansa 192.168.10.151 Search from Manage > Alerts/Notifications > Reports
2015-03-30 19:11:25 Search somansa 192.168.10.151 Search from Manage > Alerts/Notifications > Reports

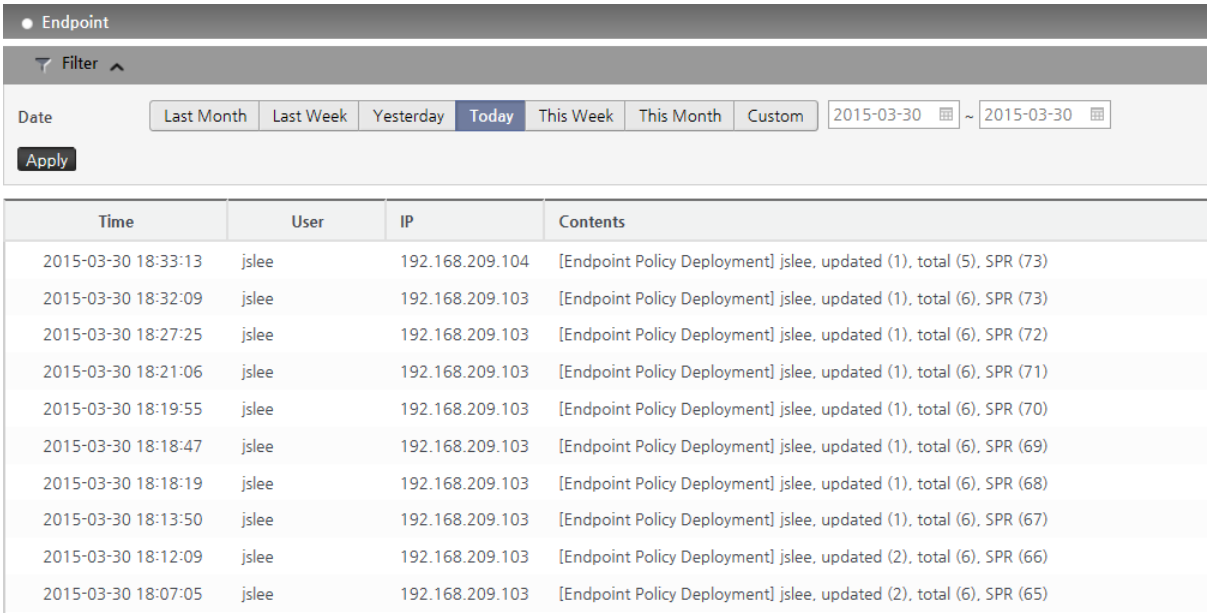
(FIGURE 4-50) AUDIT LOGS

4.6.1.1 System Logs

- Endpoint

  Records the audit logs for login and logout and policy distribution of Privacy-i Agent connected to the Privacy-i Server. In addition, logs for integrity success/failure of Privacy-i Agent can be viewed.

SOMANSA Copyright©2015 SOMANSA All rights reserved



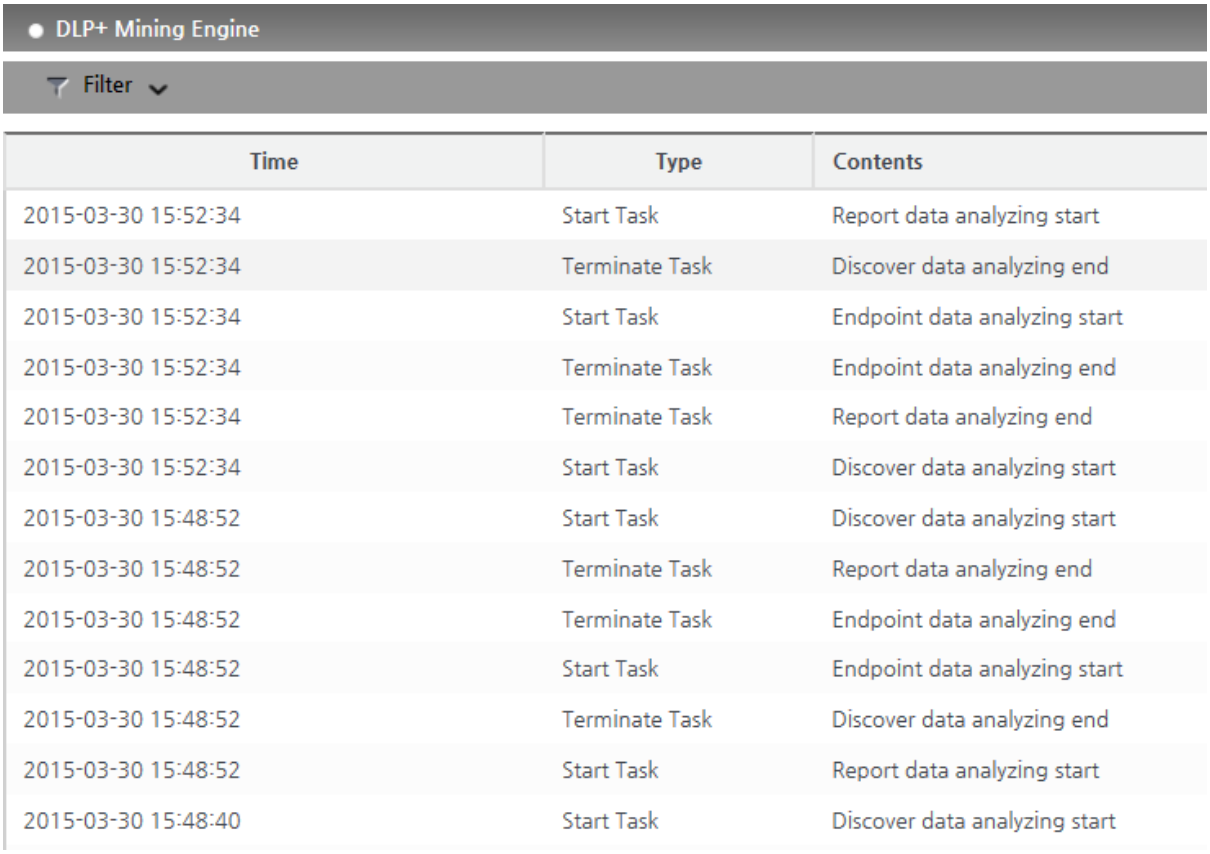
Time	User	IP	Contents
2015-03-30 18:33:13	jslee	192.168.209.104	[Endpoint Policy Deployment] jslee, updated (1), total (5), SPR (73)
2015-03-30 18:32:09	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (1), total (6), SPR (73)
2015-03-30 18:27:25	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (1), total (6), SPR (72)
2015-03-30 18:21:06	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (1), total (6), SPR (71)
2015-03-30 18:19:55	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (1), total (6), SPR (70)
2015-03-30 18:18:47	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (1), total (6), SPR (69)
2015-03-30 18:18:19	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (1), total (6), SPR (68)
2015-03-30 18:13:50	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (1), total (6), SPR (67)
2015-03-30 18:12:09	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (2), total (6), SPR (66)
2015-03-30 18:07:05	jslee	192.168.209.103	[Endpoint Policy Deployment] jslee, updated (2), total (6), SPR (65)

(FIGURE 4-51) ENDPOINT LOGS

- DLP+ Mining Engine

  Runs Mining Engine to collect Discover and Endpoint audit logs as information used on DLP+ Center at a scheduled time.

SOMANSA Copyright©2015 SOMANSA All rights reserved



Time	Type	Contents
2015-03-30 15:52:34	Start Task	Report data analyzing start
2015-03-30 15:52:34	Terminate Task	Discover data analyzing end
2015-03-30 15:52:34	Start Task	Endpoint data analyzing start
2015-03-30 15:52:34	Terminate Task	Endpoint data analyzing end
2015-03-30 15:52:34	Terminate Task	Report data analyzing end
2015-03-30 15:52:34	Start Task	Discover data analyzing start
2015-03-30 15:48:52	Start Task	Discover data analyzing start
2015-03-30 15:48:52	Terminate Task	Report data analyzing end
2015-03-30 15:48:52	Terminate Task	Endpoint data analyzing end
2015-03-30 15:48:52	Start Task	Endpoint data analyzing start
2015-03-30 15:48:52	Terminate Task	Discover data analyzing end
2015-03-30 15:48:52	Start Task	Report data analyzing start
2015-03-30 15:48:40	Start Task	Discover data analyzing start

(FIGURE 4-52) DLP+ MINING ENGINE LOGS

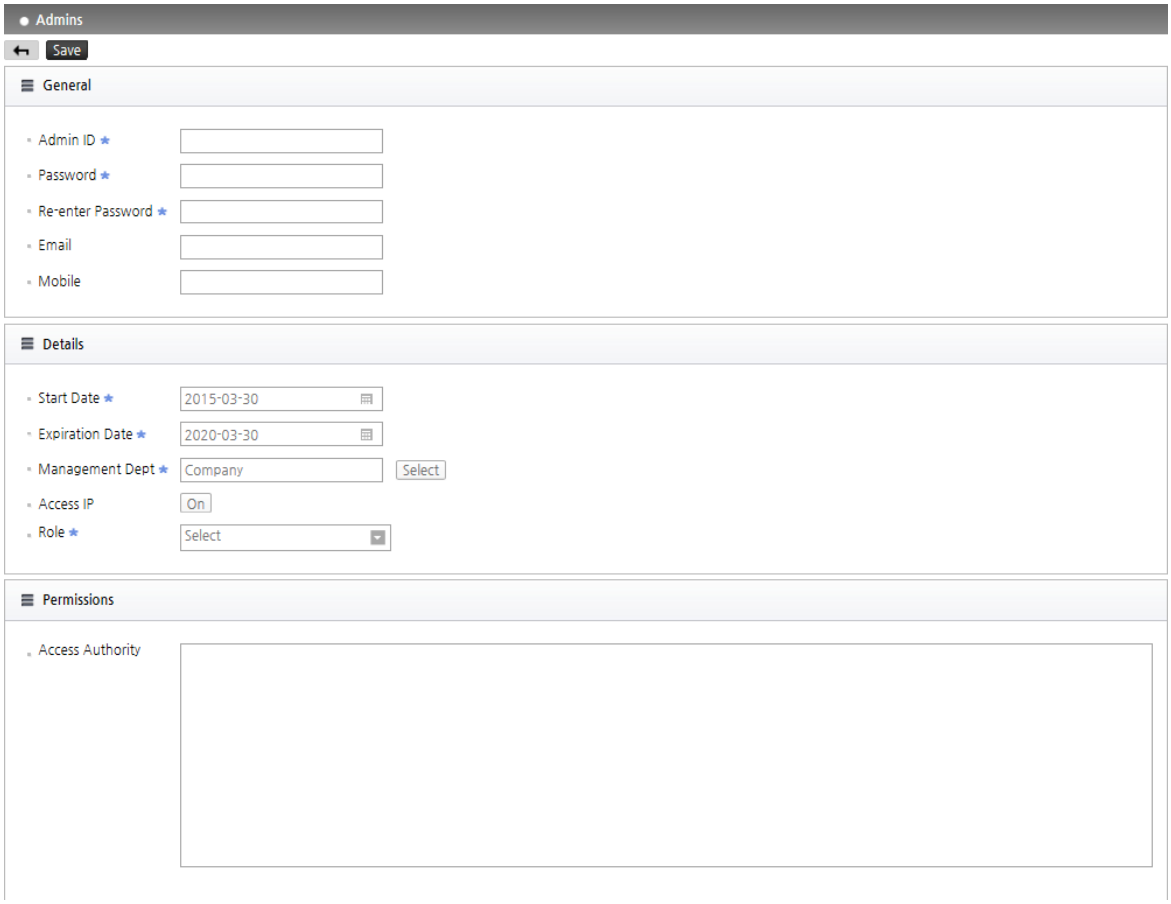
4.6.2 Admin

An admin account has the right to operate and manage the DLP+ Center. An admin account is created by the operating system admin when installing the product package. In addition, an admin can create and delete an Operator or Viewer Account according to the access department and view permissions. However, an admin account created during package installation cannot be deleted. [Table 4-21] provides a description of the account permission of DLP+ Center.

[TABLE 4-21] INTEGRATED ACCOUNT RIGHTS

Account	Rights	Number of Account
Admin	All rights, Operator and viewer account management	1
Operator	Authorized access menu and log view in a department	1
Viewer	Limited access menu and log view in a department	5

SOMANSA Copyright©2015 SOMANSA All rights reserved



(FIGURE 4-53) ADMIN REGISTRATION SCREEN

☞ Effective Input Field Range

[TABLE 4-22] EFFECTIVE INPUT FIELD RANGE WHEN REGISTERING ADMIN

Item	Effective Range	Character	Failure Message
Admin ID	5~20	English letters	An admin ID should have at least 5 characters.
Password	9~35	Numbers, uppercase/ lowercase letters, special characters	Enter password.
Re-enter Password	9~35	Numbers, uppercase/ lowercase letters, special characters	There is no password confirmation value.
Email	1~200	Numbers, uppercase/ lowercase letters, special characters	-

SOMANSA Copyright©2015 SOMANSA All rights reserved

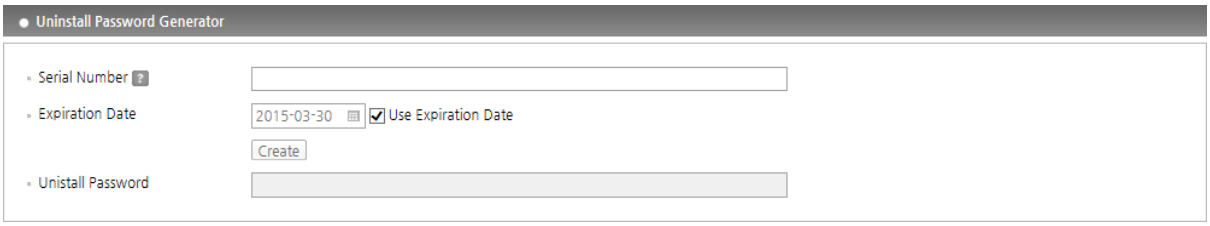
Recommendations

✓ The password must be created with more than 9 characters, including English letters, numbers and special characters

4.6.3 Tools

4.6.3.1 Uninstall Password Generator

Enter the serial number sent by an agent to generate the agent [Uninstallation Password].



(FIGURE 4-54) UNINSTALL PASSWORD GENERATOR

4.6.4 View Privacy-i Version

This screen shows the version of the DLP+ Center. Click the Info button at the top right to check the version.

(FIGURE 4-55) VIEW DLP+ CENTER VERSION

SOMANSA Copyright©2015 SOMANSA All rights reserved

5. Uninstalling Privacy-i

If Privacy-i V5.0 HyBoost needs to be uninstalled, please contact SOMANSA Support Team.

SOMANSA Copyright©2015 SOMANSA All rights reserved

6. FAQ

Q) What is an endpoint DLP solution?
A) A tool that automatically detects sensitive data on a PC, which is designated to be blocked or deleted according to current regulatory compliance and internal security policies.

Q) What types of information can an endpoint DLP solution detect?
A) Sensitive data including social security numbers, account numbers, credit card numbers, cell phone numbers, Intellectual Property, other data based on specific keywords, files, etc. can be detected.

Q) From which file types can an endpoint DLP solution detect confidential data?
A) It can detect confidential data in MS Office/HWP/pdf/txt/html/rtf/csv/other text formats.

Q) What are the criteria of a confidential data document?
A) Any information that is classified as sensitive company data or can identify individuals including customers and employees, all documents that contain account numbers, credit card numbers, social security numbers and cell phone numbers are considered confidential data documents.

Q) How can I search confidential data in a PC using an endpoint DLP?
A) Click the Privacy-i icon (confidential data detection solution) in desktop.

Q) What is Periodical Inspection (Inspection by Admin)?
A) A scheduled activity to check whether employees retain any confidential data that must be deleted. A user can view the results through a notification message such as Start Inspection / Running / Inspection Completed.

Q) How can I postpone an inspection when running Periodical Inspection (Inspection by Admin)?
A) Select the 'Run Later' button in the notification window. However, a request popup window will appear periodically.

Q) Endpoint DLP is not running.
A) It only runs when it is connected to the company network or is not currently running Periodical Inspection (Inspection by Admin).

Q) How can I check a confidential data file detected on my PC?
A) You can check depending on if you are running a Periodical Inspection (Inspection by Admin) or Inspection by User when you check confidential data extracted logs. Please see the relevant pages for more information.

SOMANSA Copyright©2015 SOMANSA All rights reserved

Q) How do I stop a Periodical Inspection (Inspection by Admin)?
A) You cannot stop a Periodical Inspection (Inspection by Admin) in progress. However, you can stop an inspection with the "Stop Inspection" button if it is being run by a user.

Q) How do I view which confidential data content exists in an extracted confidential data file?
A) You can view confidential data details through the "View File Details" menu, which appears when you select the file on the View Log List and right-click.

Q) I need a description of the function buttons on the View Log List screen after inspection is completed.
A) The functions include Select All, Move, Delete, Statistics and Reports. Please see the relevant pages for detailed instructions.

Q) What should I do if a confidential data file is detected?
A)① For a file needed for business, specify it as "General (Business)" in the confidential data categorization menu, and make sure to delete it when the task is completed. ② For a file related to personal life, specify it as "Private (Personal)". ③ For a detection error that does not contain confidential data, specify it as "Exception File". ④ Other files must be completely deleted. When storing a confidential data file in a PC, you must encrypt the file and completely delete files specified for business after the task is completed.

Q) How do I completely delete a detected file?
A) Select the file to delete in the View Log List, and click the "Delete" button.

Q) I opened the detected confidential data file, but there are no confidential data.
A) This may occur when detection information is hidden, chart/graph is linked (OLE, Object Linking and Embedding), or detection error is matched to the confidential data pattern. Please see the relevant pages for more information.

Q) What does "Other Detection" mean in the View Log after inspection is completed?
A) Other Detection means it is unable to check content due to an encrypted file through a self-encrypting function (ex: MS Office, ZIP password settings, etc.)

Q) I ran Periodical Inspection (Inspection by Admin). What happens to the results?
A) Periodical Inspection (Inspection by Admin) results can be checked by a user on a PC. In addition, the summary statistics by team/user (number of detections) are automatically sent to an administrator by E-mail. An administrator needs to check the detected data content and continuously delete unnecessary confidential data.
※ When running an inspection by a user, an E-mail will not be sent and only the user can check

SOMANSA Copyright©2015 SOMANSA All rights reserved

the results.

Q) How do I re-run the user information input window if the user information was not entered during the agent installation?
A) Restart your PC to re-run.

Q) What is the key-shaped icon in the lower-right corner of my desktop after the final installation?
A) The information window of the agent icon is configured with 6 menus, including Running Privacy-i, View Policy, View Event Log, Policy Update, Module Update and Re-login.

Q) How do I uninstall the confidential Endpoint DLP (Privacy-i Agent)?
A) A user cannot arbitrarily uninstall the Privacy-i Agent. If uninstallation is needed, please contact a SOMANSA engineer.

Q) Is there a function for preventing the unauthorized access of a server and client?
A) There is an xml-based command protocol which is defined by the SOMANSA product through a TCP/IP-based server service communication port. When a service communication port of the unauthorized server connects and transfers a random dummy string, this will be ignored by the server service. For a client which is used by an admin, the account will be automatically locked for a certain period of time when login authentication fails 5 times. In addition, if the same account is connected to the client simultaneously in two places, the prior connection will be automatically shut down with an alert message.

Q) What should I do when a server's operating system and hardware fails, other server functions fail, and server recovery is needed due to a user error?
A) Report the failure and request maintenance support at the SOMANSA Help Desk. After receiving a remote or on-site inspection, please take action, such as patching the module, updating or re-installing the product depending on the inspection results of the engineer.

Q) Do you provide a function to check an event regarding product error or the cause of an error?
A) If an error such as abnormal termination of service and program termination occurs, please check the event logs of your operating system. For the detailed inspection for an error, we recommend you to receive an inspection through the SOMANSA Help Desk Request and Inquiries for On-Line/Off-Line support.

SOMANSA Copyright©2015 SOMANSA All rights reserved

7. Definition of Terms

Account Management Log

Added, modified and deleted logs of an admin account and identified and approved logs of an authorized admin

Viewer

Has permission to audit logs for modified history of the DLP+ Center (restricted access right)

Audit(Security) Log

Audit logs stored in the database while running security functions in the DLP+ Center. Refers to Information Management Log, Policy Management Log, Account Management Log, System Log, etc.

User

Refers to anyone who uses a PC with the agent installed in a company.

User Data

Data generated for a user by a user that does not affect product operation.

Identity

Identifies an authorized user.

System Administrator

An authorized admin who is in charge of product operation and preferences in the control panel.

SOMANSA Copyright©2015 SOMANSA All rights reserved

System Log

An updated log on policies and patterns

Administrator

Has the right to edit policy in the DLP+ Center.

Agent

Is installed on a user PC, and operates only in the Windows/Linux environment. Runs a scan when an agent user inspects confidential data on their own PC, or when an administrator forcefully scans confidential data on a user PC from the server.

DBMS

A DB server where all audit logs are stored. PostgreSQL is selected and used for this product.

External Interface

A general term for various ports that can leak data stored in the host. It includes USB, IDE, SATA, e-SATA, IEEE1394, PCMCIA, LAN/WLAN, Bluetooth, Serial/Parallel Port, Infrared port, etc.

Threat Agent

An unauthorized user/admin or external IT entity that poses threats such as illegal access, modifying and deleting assets.

Authorized Administrator

Refers to the System Administrator, Admin, Operator and Viewer.

SOMANSA Copyright©2015 SOMANSA All rights reserved

Authentication Data

Information used to verify the identity of a user.

Operator

A person who can view all audit data, and add/delete/modify policy/pattern among authorized administrators

Information Management Log

Edit Log / Statistic Report Output Log of a PC user in a company who uses a user PC log collected through the agent and History Log/Agent that the admin checks Policy Management

Policy Management Log

Log with pattern/policy edited by an admin and an operator.

Organizational Security Policy

Security rules, procedures, practices, guidelines, etc. which are enforced by the organization

Content

Various information or content that are stored in the host or provided through a network. Can be expressed in a particular file format (HWP, TXT, DOC, PDF, DOCX, PPT, PPTX, XLS, XLSX, ZIP, etc.) and can be information itself.

DLP+Center

An administration console that an admin/operator/viewer can log into, in order to set confidential data patterns policy rules, view reports, and register agent users, etc.

SOMANSA Copyright©2015 SOMANSA All rights reserved

Protocol

Communication rules to provide user services such as E-mail, Messenger, File Upload • Download and Web. Generally refers to SMTP, HTTP, HTTPS, FTP, SFTP, SSH, TELNET, IMAP, IRC, RDP, etc.

SOMANSA Copyright©2015 SOMANSA All rights reserved